EXHIBIT A

From:	Ronald Abramson
To:	Kris Leftwich; TDN Plaintiff
Cc:	TDN Defendants; Ari J. Jaffess; Alex G. Patchen; David G. Liston; Megan Leicht; dfinger@delawgroup.com
Subject:	RE: TDN Litigation - Rebuttal Expert Declaration - Case Nos. 1:19-01062-CFC-CJB, 1:19-01063-CFC-CJB, and 1:19-01064-CFC-CJB
Date:	Monday, February 1, 2021 12:34:54 PM
Attachments:	Rowe Dec. 2021-01-28.pdf

*** EXTERNAL EMAIL ***

Counsel, attached is the Declaration of Anthony Rowe, which addresses a discrete point first raised in the reply declaration referenced below.

Best regards,

Ron Abramson

From: Kris Leftwich <KLeftwich@chenleftwich.com>
Sent: Wednesday, December 30, 2020 5:15 PM
To: TDN Plaintiff <TDNPlaintiff@chenleftwich.com>
Cc: TDN Defendants <TDNDefendants@chenleftwich.com>
Subject: TDN Litigation - Rebuttal Expert Declaration - Case Nos. 1:19-01062-CFC-CJB, 1:19-01063-CFC-CJB, and 1:19-01064-CFC-CJB

Counsel,

The attached rebuttal declaration of Dr. Michael Caloyannides is being served pursuant to the Section 101 scheduling order in Case Nos. 1:19-01062-CFC-CJB, 1:19-01063-CFC-CJB, and 1:19-01064-CFC-CJB. Exhibit A to the declaration is provided in two versions: (1) original, locked PDF file and (2) labeled exhibit.

Please contact me if you are unable to access any of the materials.

Best,
Kris

Kristoffer Leftwich
Partner

Chen Leftwich LLP
1700 Pacific Ave.
Ste. 2400
Dallas, TX 75201

Office: 214-627-9970
Mobile: 214-909-6512
KLeftwich@ChenLeftwich.com

EXHIBIT B

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

TRIDINETWORKS LTD., Plaintiff, v. NXP-USA, INC. and NXP B.V., Defendants.	No. 1:19-01062-CFC-CJB
TRIDINETWORKS LTD., Plaintiff, v. SIGNIFY NORTH AMERICA CORPORATION and SIGNIFY NETHERLANDS B.V., Defendants.	No. 1:19-01063-CFC-CJB
TRIDINETWORKS LTD., Plaintiff, v. STMICROELECTRONICS, INC., and STMICROELECTRONICS INTERNATIONAL N.V., AND DOE-1 d/b/a "STMICROELECTRONICS," Defendants.	No. 1:19-01064-CFC-CJB

DECLARATION OF MICHAEL CALOYANNIDES, PH.D. CONCERNING THE CONVENTIONAL APPLICATION OF COMPUTER TECHNOLOGY IN THE CLAIMS OF THE '276 PATENT

network to a device being installed in the network. Configuration has long been required for network operation.

b. Commissioning Tool

35. In the installation step of claim 1, "accessing the created design" is performed "by a commissioning tool." Claim 1 does not say what a commissioning tool is, and the specification of the patent defines it in purely functional terms as "a (usually portable) unit used to deploy and configure devices." '276 Patent 9:44-46. The '276 Patent suggests that a commissioning tool might take the form of a PDA, or personal digital assistant, to "access/download and use the design data created in the design system." '276 Patent 13:1-6. Prior to November 2007, a PDA was a well-known, conventional computer technology for accessing and downloading data.

c. Configuration Adapter Comprised in a Device Being Configured

36. In the installation step of claim 1, data is downloaded "from said commissioning tool into a configuration adapter comprised in said devices." Once again, claim 1 does not say what a configuration adapter is, and the specification of the '276 Patent only defines it in purely functional terms as "a component in a device or connected to a device which receives and stores configuration data." '276 Patent 9:48-50. This definition suggests only that a configuration adapter includes a memory, but computer memory was a conventional computer component prior to

November 2007, and storing data was the conventional computer operation performed by a memory prior to November 2007.

37. The '276 Patent also states repeatedly that "[t]he download may be carried out by contactless technologies (such as RFID/NFC)." '276 Patent 4:25-28, 13:35-37, 13:66 – 14:1, 14:38-40, 14:58-60. RFID and NFC were well-known, standardized, and conventional computer technologies before November 2007.[3] In addition, the prior art discloses several RFID/NFC devices with memories capable of receiving information via a contactless transmission and storing that information in memory. (*See* section V.D of this declaration for a discussion of the multiple interface memory card of the Spencer Patent and the ID tag of the Teraura Patent; *see also* section V.E of this declaration for a discussion of the RFID tag of the Smith Patent and the RFID module of the Dua Patent.) In fact, some of those devices were specifically used to receive and store network configuration information. (*See* section V.E of this declaration for a discussion of the RFID tag of the Smith Patent and the RFID module of the Dua Patent.) Accordingly, a POSITA would have considered the configuration adapter recited in claim 1 to be a conventional computer component prior to November 2007.

[3] For a detailed discussion of RFID and NFC, refer to section V.C of this declaration.

i. TDN's Allegations that Configuration Adapters are Unconventional Computer Components

38. I am informed that TDN asserts that a configuration adapter, as illustrated in Figure 7 of the '276 Patent, includes features not available in conventional technology before November 2007. For example, TDN refers to the illustration of Figure 7 and alleges that such a configuration adapter "has 'dual' (two-sided) interfaces, to be able to share data between *both* an external commissioning tool (*e.g.*, via wireless) on one end of the adapter, and, then or later, with other electronic components wired to the adapter (*e.g.*, on-board processor circuitry), on the other end of the adapter." First Amended Complaint for Patent Infringement, Case 1:19-cv-01064-CFC-CJB, D.I. 55 ¶ 24 (July 13, 2020) (emphasis in original). TDN also alleges that "[a]s of the date of invention of the '276 Patent (which was at least as early as its first filing date in November 2007) there did not exist a commercially available persistent storage device providing both a communication and a device contact interface, as in the configuration adapter of the '276 Patent . . . ." First Amended Complaint for Patent Infringement, Case 1:19-cv-01064-CFC-CJB, D.I. 55 ¶ 30 (July 13, 2020).

39. I disagree with TDN's assertions about the availability of features illustrated in Figure 7 of the '276 Patent for a variety of reasons, including because those features were described in numerous prior art references as discussed in this declaration. For example, U.S. Patent No. 6,712,277 ("Spencer" or "Spencer Patent")

was titled "Multi Interface Memory Card" and described a memory card with both a wireless NFC interface (according to ISO 14443-2) and a wired interface. The application for the Spencer Patent was filed on December 5, 2001. See section V.D.1 of this declaration for a full analysis of the Spencer Patent. U.S. Patent No. 6,873,259 ("Teraura" or "Teraura Patent") was published in March 2003 and disclosed an ID tag that included a memory, a wireless RF interface, and a wired interface. See section V.D.2 for a full analysis of the Teraura Patent. The Smith Patent, mentioned previously in this declaration, disclosed an RFID tag with a memory and an additional wired interface, and it was used to receive and store network configuration data. The Smith Patent arose from an application filed in August 2006. See section V.E.1 for a full analysis of the Smith Patent. Similarly, U.S. Patent No. 8,244,179 ("Dua" or "Dua Patent"), which published in November 2006, disclosed an RFID tag with a memory and an additional wired interface for exchanging configuration data for establishing wireless communications. See section V.E.2 of this declaration for a full analysis of the Dua Patent.

40. Put simply, a device combining an RFID/NFC interface and a wired interface was a conventional computer component before November 2007, and more specifically, a configuration adapter combining both interfaces was a conventional computer component before November 2007.

41. I also disagree with TDN's assertions about the availability of features illustrated in Figure 7 of the '276 Patent because TDN's assertions are contradicted by the disclosures of the '276 Patent, itself.

42. The '276 Patent describes Figure 7 as follows: "FIG. 7 is a schematic block diagram of a configuration adapter 204, according to the present invention." '276 Patent 14:47-48. That is all Figure 7 is: a block diagram. As shown below, Figure 7 illustrates configuration adapter 204 as a combination of **three functional blocks**. It does not identify or illustrate any of the electronic components one might use to produce a configuration adapter or any of the three functional blocks.

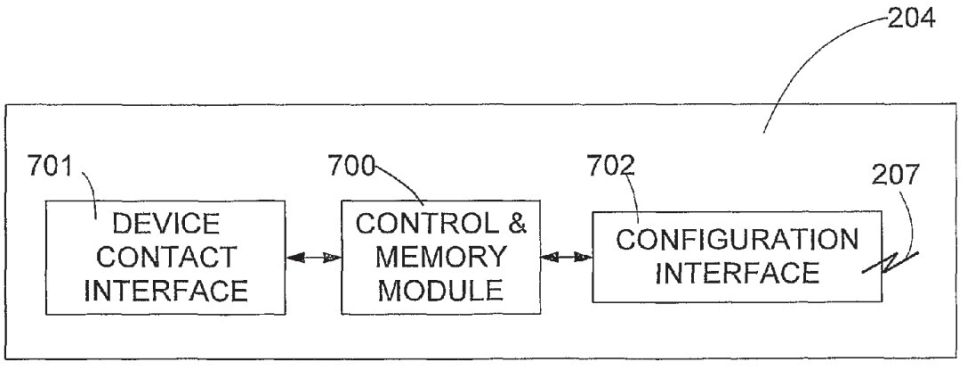


Fig. 7

43. Each block within Figure 7 is labeled in purely functional terms. For example, block 701 is labeled "device contact interface," which is presumably a communication interface involving device contact. The label "device contact interface" merely describes the use or function of that block. It does not identify a

particular type of interface or electronic component. Similarly, block 710 is labeled "configuration interface," which is presumably a communication interface used for configuration. Again, the label describes a use or function, not a particular type of interface or electronic component. The same is true of block 700, labeled "control & memory module." Obviously, the purpose of this block is to perform control and memory functions, but the label does not specify the design or structure of the block. For example, it does not specify a type of controller – general-purpose CPU, application-specific integrated circuit (ASIC), field programmable gate array (FPGA), etc. Nor does it specify a type of memory – RAM, ROM, flash memory, register memory, etc. It also does not specify whether the "module" is comprised of individual components assembled on a circuit board or whether it is comprised of a single integrated circuit, known as a microcontroller. Any or all of these implementations are consistent with a purely functional illustration like Figure 7, and all of these implementations were well-known to a POSITA before November 2007.

44. Most importantly, Figure 7 does not illustrate or even suggest a new type of electronic component. Communication interfaces, both wired and wireless, were well-known in the art long before November 2007. Ascribing a use or function to the interface – e.g., "device contact" or "configuration" – does not identify or require a new type of electronic interface. It merely describes a use to be made of an

existing interface. The same is true of the "control & memory module." As discussed in the previous paragraph, many, many options for implementing a control & memory module would have been known and available to a POSITA before November 2007.

45. My observations in this regard are confirmed directly by the specification of the '276 Patent. In describing Figure 7, the '276 Patent makes it absolutely clear that Figure 7 is nothing more than an assembly of well-known electronic components performing their well-known functions as understood by a POSITA before November 2007.

46. For example, the '276 Patent admits that "[t]he device contact interface 701 may be a **standard** communication interface (such as SPI or 1-Wire) or a **standard** control interface (such as DALI[4])." '276 Patent 14:67 – 15:1 (emphasis added). The '276 Patent does not provide any further explanation or description of device contact interface 701. Notably, it does not disclose or suggest that a standard interface must be modified in any way in to implement device contact interface 701. It should go without saying, but the structure, function, and operation of a **standard** interface would be known to a POSITA before November 2007. Thus, device contact

[4] "DALI" is an acronym for digital addressable lighting interface, '276 Patent 12:33-36, a wired communication interface standardized in Europe.

interface 701 must be a conventional electronic component performing a conventional function as understood by a POSITA before November 2007.

47. In discussing Figure 7, the '276 Patent also plainly states that "configuration interface 702 implements identical configuration link communication protocols (such as **ISO 14443**)." '276 Patent 14:53-57 (emphasis added). ISO 14443 is the **international standard** that defines and specifies the operation of devices implementing near field communications.[5] Notably, the '276 Patent does not describe or suggest any modification to the protocols specified by ISO 14443. Thus, according to the '276 Patent, configuration interface 702 is nothing more than NFC, and NFC was standardized and available for commercial application as of July 2001. It should go without saying, but the structure, function, and operation of a **standard** interface would be known to a POSITA before November 2007. Thus, configuration interface 702 must be a conventional electronic component performing a conventional function as understood by a POSITA before November 2007.

48. Finally, in discussing Figure 7, the '276 Patent says almost nothing about control & memory module 700. It says only that "[t]he control and memory module 700 may be used to store the loaded configuration data and to control the

[5] For a detailed discussion of ISO 14443, refer to sections V.C.2 - V.C.5 of this declaration.

adapter." '276 Patent 14:60-61. Nothing more is said about the structure or operation of control and memory module 700 in the entire specification of the '276 Patent. In fact, the specification of the '276 Patent says **nothing at all** about the **structure** of control and memory module 700. It certainly does not suggest that control and memory module 700 is made up of unconventional or non-standard components. Indeed, the only functions attributed to control and memory module 700 – storing data and performing control[6] – were conventional functions of conventional memory and microprocessors known to a POSITA before November 2007. They are also conventional functions of conventional microcontrollers (which combine processing, memory, and I/O functions in a single integrated circuit) known to a POSITA before November 2007.

49. To the extent that TDN argues that control and memory module 700 is unconventional because Figure 7 shows it has connections to two types of interfaces,[7] the disclosures of the '276 Patent simply do not bear this out. The specification does not discuss, describe, or even suggest making any modifications

[6] '276 Patent 14:60-61 ("The control and memory module 700 may be used to **store** the loaded configuration data and to **control** the adapter." (emphasis added)).

[7] First Amended Complaint for Patent Infringement, Case 1:19-cv-01064-CFC-CJB, D.I. 55 ¶¶ 24, 30 (July 13, 2020) (emphasis in original).

to conventional components to achieve connections to both interfaces. In fact, the specification of the '276 Patent does not discuss the structure or composition of control and memory module 700 at all. This is notable, because one would expect some – probably even significant – discussion if unconventional components were required to implement a feature of the patented invention. The fact that the '276 Patent is silent on this point speaks volumes to a POSITA.

d. Downloading Configuration Data Before a Device is Initialized

50. The installation step of claim 1 also recites that configuration data is downloaded into the network devices "before the devices are initialized." Before November 2007, a POSITA would have considered this to be a conventional application of computer technology. In fact, Intel's Smith Patent describes this exact application of RFID technology. See section V.E.1 for a full analysis of the Smith Patent. By way of summary, Intel's Smith Patent discloses the use of "a radio frequency identification (RFID) tag to wirelessly receive configuration parameters for another device and store those parameters in a non-volatile storage element, **even if the device is powered off and even if the device is still in its shipping carton at the time.**" Smith 2:48-53 (emphasis added). Smith further explains: "At a later time, when the device is powered up, the device may read those parameters from the

193. The RFID module of Dua implemented computer technologies and operated according to industry standards and principles that were already conventional by the time the application for the Dua Patent was filed. By November 2007, a POSITA would consider the RFID module of Dua, and the manner and method of its operation, to be an example of conventional computer technology.

VI. Conclusion

194. The foregoing represents my opinions to date, but I reserve the right to supplement my opinions in response to arguments raised in opposition to this declaration or if further evidence or information becomes available.

195. I declare under penalty of perjury that the foregoing is true and correct.

Dated: November 4, 2020

Michael Caloyannides, Ph.D.

EXHIBIT C

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

TRIDINETWORKS LTD., Plaintiff, v. NXP-USA, INC. and NXP B.V., Defendants.	No. 1:19-01062-CFC-CJB
TRIDINETWORKS LTD., Plaintiff, v. SIGNIFY NORTH AMERICA CORPORATION and SIGNIFY NETHERLANDS B.V., Defendants.	No. 1:19-01063-CFC-CJB
TRIDINETWORKS LTD., Plaintiff, v. STMICROELECTRONICS, INC., and STMICROELECTRONICS INTERNATIONAL N.V., AND DOE-1 d/b/a "STMICROELECTRONICS," Defendants.	No. 1:19-01064-CFC-CJB **Declaration of Anthony G. Rowe**

I, ANTHONY G. ROWE, declare the following under penalty of perjury:

1. I have been retained by counsel for Patent Owner TriDiNetworks Ltd. ("TDN") to provide my opinions on certain issues raised by the defendants' contentions in these cases that

my opinion is unsupported and incorrect, that, in addition to possessing the foregoing qualifications, a POSITA would *also* have "two to five years of experience in the design, operation, or application of active and passive RFID or NFC devices." (Report at ¶ 21.) In my opinion, the addition of RFID or NFC experience is a wholly unrealistic expectation for the qualifications of a POSITA in late 2007.

39. As of late 2007 (and as I address in further detail later in this Report, at ¶¶ 64-67), a POSITA in the field of the '276 patent would not have had *any* substantive experience with NFC technologies. This is particularly true for NFC technologies that can read and store information in the manner contemplated in the '276 patent, which were not then in any commercial use, especially with respect to home/industrial automation. Such technologies (such as dual-interface EEPROMs) did not become commercially available until about 2010, as reflected, for example in STMicroelectronics, Inc.'s own M24LR64 device, introduced in 2010 (*see* Exhibit D). Consequently, no POSITA could have had the "two to five years of experience" in such NFC technologies as contemplated by Dr. Caloyannides. Indeed, it is only recently that POSITAs are becoming familiar with and using such NFC technologies for network setup and configuration purposes.

IV. *ALICE* STEP ONE

40. Dr. Caloyannides characterizes the claims of the '276 patent as "nothing more than an abstract way to describe the design of any computer network – configuration plus connections." (Report at 24.)

41. Based on my understanding of the necessary analysis under step one of *Alice*, it is my view that Dr. Caloyannides' formulation is an overly abstract and inadequate statement of the character of the claims. It is simply a statement of the subject area addressed by the claims, and

conventional did change the result. Dr. Caloyannides extensively discusses "conventionality" in his *Alice* step one analysis, which appears to me more like an obviousness argument than one directed at the proper tests under *Alice*.[4]

62. Second, in any case, I would not agree by any means that a "configuration adapter" as described in the '276 patent was a "conventional" item in the field of the '276 patent as of November 2007. Today, as shown in Exhibits E and F hereto, one can readily buy such items, referred to as dual-interface NFC EEPROM chips, from suppliers, such as NXP USA, Inc. (e.g., its NTAG-I2C of chips) and STMicroelectronics, Inc. (e.g., its M24LR family of chips) (though I would not say that their use to configure automation devices has become conventional, even today). However, as already noted, these devices did not appear on the market until approximately 2010. *See* Exhibit D hereto. In 2007, such items were not generally available off-the-shelf.

63. As I understand the applicable law, the question of whether a configuration adapter would be considered a "routine or conventional" device to use in the field of network automation as of November 2007 could bear on *Alice* step two, in the event the Court found it necessary to address step two. By no stretch could such technology have been considered to have become "routine or conventional" in such applications by that date.

64. While it may be fair to say that *communication* over RFID in general was widely known in electrical engineering as of 2007 (for example, the merchandise tags in a retail store), the '276 patent requires more than the mere application of RFID communication to solve a problem that was theretofore approached without it. The solution disclosed in the '276 patent also requires application of a deeper capability of RFID, that of using the RFID signal also to

[4] I also disagree with Dr. Caloyannides to the extent his arguments concern obviousness, for the reasons I previously expressed in the IPR proceeding.

interactions are met. Dr. Caloyannides' formulation seems to be inappropriately broad for purposes of *Alice* step one.

91. In sum, Dr. Caloyannides' Report begins with an overly broad formulation of the alleged abstract idea of the '276 patent claims, shortcuts the analysis under step one by failing to identify what the patent regards as distinguishing its claims from the prior art, and then proceeds immediately to step two, based on the alleged conventional nature of the items used to practice the individual process steps, overlooking the characteristics of the underlying process itself, as well as any ordered combination of the claim elements. In addition, it repeatedly seeks to establish the alleged conventional nature of the items used in the process by finding similar examples somewhere in the prior art, without further support for what is conventional, whereas, as I understand the law, merely being identified in the prior art is not sufficient to show that an item is routine and conventional for purposes of patent-eligibility.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on December 4, 2020.

ANTHONY G. ROWE

EXHIBIT D

Press Releases

Press Release

View printer-friendly version

<< Back

STMicroelectronics Launches New Dual-Interface EEPROM Enabling Remote Access to Electronic Device Parameters

New RFID-compatible EEPROMs simplify lifetime management and enable new features and capabilities

GENEVA, March 2, 2010 /PRNewswire via COMTEX/ -- STMicroelectronics (NYSE: STM), a world leader in RF Memory and EEPROM ICs, has announced sample availability of the first in a new family of products that provide the flexibility to remotely program or update electronic products, anytime during their lifetime, and anywhere in the supply chain. The new devices enable manufacturers to update parameters, regionalize or activate software without connecting a programmer, or even opening the retail packaging. This pioneering way to access the memory will allow businesses to add new functions and capabilities to their products, but also reduce manufacturing costs, simplify inventory management, and respond more quickly to changing market demands.

The M24LR64 is an EEPROM memory with a standard I2C serial interface, providing communication with most microcontrollers or ASICs, and also a standard ISO15693 RF (radio frequency) interface for wireless communications with RFID readers. The ISO15693 standard is passive RFID technology, which gathers both the energy and the data from the RF system. No power is required to operate the M24LR64 in RF mode, which enables on-board energy savings and provides easy and convenient remote access to electronic product parameters.

"This highly innovative ability to program or read a memory wirelessly, as well as electrically, will provide tremendous added-value to our customers, enabling highly flexible supply-chain management and also stimulating new types of products with powerful features and capabilities," said Benoit Rodrigues, General Manager, Memories Division, STMicroelectronics. "Moreover this new memory is compatible with existing RFID equipment, thereby delivering a wide range of solutions and an accessible technology to product manufacturers"

Based on two industry-standard interfaces, the new dual-interface product line provides a link between the operation of electronic devices and the RFID world. This will enable new types of products, including those requiring asset tracking, data collection, diagnostics, or traceability, such as medical devices, industrial equipment, and automotive electronics. Computer peripherals and consumer products will take advantage of the M24LR64 feature set for easy and convenient parameter and regional setting update, even when the device is in its package seal. Also, RFID systems requiring additional monitoring, such as cold-chain verification, will also benefit from the high memory density of the M24LR64.

The M24LR64 has a 64-Kbit capacity for storage of program code, product parameters, serial numbers, calibration data, or event-log data. Its RF ISO15693 interface can be accessed by a wide range of RF readers, covering hand-held devices, pad antennas, gate systems and tunnel readers. The memory also communicates with the host system via an industry-standard I2C interface operating at 400kHz from 1.8 to 5.5V. It also comes with a unique and flexible 32-bit password protection scheme to protect the application from unauthorized tampering or to prevent unexpected access to memory.

The Dual-Interface EEPROM products can be used with either on-board or off-board antenna types in a variety of form factors, allowing product designers to optimize aspects such as overall dimensions, communication range, and pc-board complexity. The M24LR64 is available in TSSOP-8, SO-8, and MLP 2 x 3 packages, or as bare die, at prices from $0.90 for orders of 1000 pieces. Sampling has already begun, with volume production scheduled for Q2 2010. ST plans to introduce additional members of the Dual-Interface EEPROM family in the second half of 2010.

About STMicroelectronics

STMicroelectronics is a global leader in developing and delivering semiconductor solutions across the spectrum of microelectronics applications. An unrivalled combination of silicon and system expertise, manufacturing strength, Intellectual Property (IP) portfolio and strategic partners positions the Company at the forefront of System-on-Chip (SoC) technology and its products play a key role in enabling today's convergence markets. The Company's shares are traded on the New York Stock Exchange, on Euronext Paris and on the Milan Stock Exchange. In 2009, the Company's net revenues were $8.51 billion. Further information on ST can be found at www.st.com.

SOURCE STMicroelectronics

NT3H2111_2211

NTAG I²C *plus*: NFC Forum T2T with I²C interface, password protection and energy harvesting

Rev. 3.5 — 7 May 2019
359935

Product data sheet
COMPANY PUBLIC

1 General description

Designed to be the perfect enabler for NFC in home-automation and consumer applications, this feature-packed, second-generation connected NFC tag is the fastest, least expensive way to add tap-and-go connectivity to just about any electronic device.

NXP NTAG I²C *plus* is a family of connected NFC tags that combine a passive NFC interface with a contact I²C interface. As the second generation of NXP's industry leading connected-tag technology, these devices maintain full backward compatibility with first-generation NTAG I²C products, while adding new, advanced features for password protection, full memory-access configuration from both interfaces, and an originality signature for protection against cloning.

The second-generation technology provides four times higher pass-through performance, along with energy harvesting capabilities, yet NTAG I²C *plus* devices are optimized for use in entry-level NFC applications and offer the lowest BoM of any NFC solution.

I²C and NFC communications are based on simple, standard command sets, and are augmented by the demo board OM5569/NT322E, which includes online reference source code. All that is required is a simple antenna design (see Ref. 5), with no or only limited extra components, and there are plenty of reference designs online for inspiration. NTAG I²C *plus* development board is certified as NFC Forum Type 2 Tag (Certification ID: 58514).

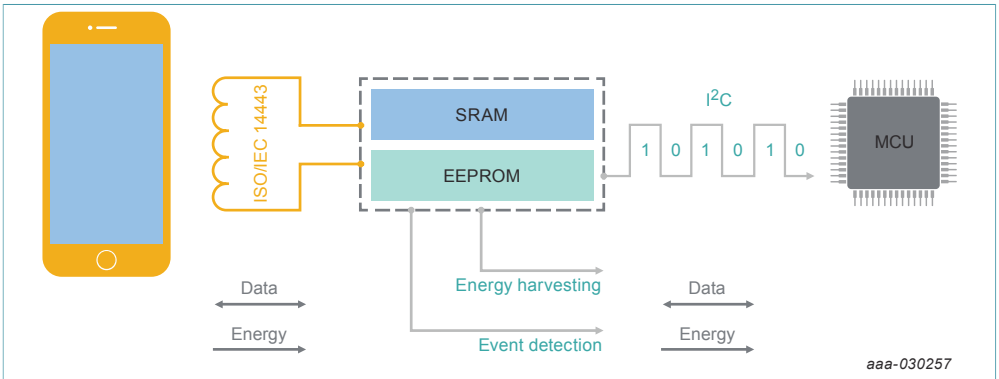


Figure 1. Contactless and contact system

2 Features and benefits

2.1 Key features

- Interoperability
  - ISO/IEC 14443 Part 2 and 3 compliant
  - NTAG I²C *plus* development board is certified as NFC Forum Type 2 Tag (Certification ID: 58514)
  - Unique 7 byte UID
  - GET_VERSION command for easy identification of chip type and supported features
  - Input capacitance of 50 pF
- Host interface
  - I²C slave
  - Configurable field detection pin based on open-drain implementation to signal NFC events or synchronize pass-through data transfer
- Memory
  - 2k bytes EEPROM
  - 64 bytes SRAM buffer for transfer of data between NFC and I²C interfaces with memory mirror or pass-through mode
  - Clear arbitration between NFC and I²C memory access
- Data transfer
  - Pass-through mode with 64 byte SRAM buffer
  - FAST_WRITE and FAST_READ NFC commands for higher data throughput
- Security and memory-access management
  - Full, read-only, or no memory access from NFC interface, based on 32-bit password
  - Full, read-only, or no memory access from I²C interface
  - NFC silence feature to disable the NFC interface
  - Originality signature based on Elliptic Curve Cryptography (ECC) for simple, genuine authentication
- Power Management
  - Configurable field-detection output signal for data-transfer synchronization and device wake-up
  - Energy harvesting from NFC field, so as to power external devices (e.g. connected microcontroller)
- Industrial requirements
  - Temperature range from -40 °C up to 105 °C

2.2 NFC interface

- Contactless transmission of data at 106 kbps
- NTAG I²C *plus* development board is certified as NFC Forum Type 2 Tag (Certification ID: 58514) (see Ref. 1)
- ISO/IEC 14443A compliant (see Ref. 2)
- Data transfer of 106 kbit/s
- 4 bytes (one page) written including all overhead in 4.8 ms via EEPROM or 0.8 ms via SRAM
- 64 bytes (whole SRAM) written including all overhead in 6.1 ms using FAST_WRITE command

- Data integrity of 16-bit CRC, parity, bit coding, bit counting
- Operating distance of up to 100 mm (depending on various parameters, such as field strength and antenna geometry)
- True anticollision
- Unique 7-byte serial number (UID) according to ISO/IEC 14443-3 (see Ref. 2)

2.3 Memory

- 2k bytes EEPROM
- 64 bytes SRAM volatile memory without write endurance limitation
- Data retention time of minimum 20 years
- EEPROM write endurance minimum 500.000 cycles

2.4 I²C interface

- I²C slave interface supports frequencies up to 400 kHz (see Section 13.1)
- Fail safe I²C operation
- I²C slave supports 7-bit slave address.
- As the least significant R/$\overline{W}$ bit is used to indicate data transfer direction, default slave address 55h recalculates to an I²C write address AAh and an I²C read address ABh respectively.
- 16 bytes (one block) written in 4 ms (EEPROM) or 0.4 ms (SRAM)
- NTAG I²C *plus* can be used as standard I²C EEPROM and I²C SRAM

2.5 Security

- Manufacturer-programmed 7-byte UID for each device
- Capability container with one time programmable bits
- Field programmable read-only locking function per page for first 12 pages and per 16 (1k version) or 32 (2k version) pages for the extended memory section
- ECC-based originality signature
- 32-bit password protection to prevent unauthorized memory operations from NFC perspective may be enabled for parts of, or complete memory
- Access to password protected data area may be restricted from I²C perspective
- Pass-through and mirror mode operation may be password protected
- Protected data can be safeguarded against limited number of negative password authentication attempts

2.6 Key benefits

- Full interoperability with every NFC-enabled device
- Smooth end-user experience with super-fast data exchange (up to 40 kbit/s) via NFC and I²C interface
- Zero-power operation with non-volatile data storage
- Energy harvesting feature delivers up to 15 mW out of NFC field to power (parts of) host system
- Data protection to prevent unauthorized data manipulation
- Multi-application support, enabled by memory size and segmentation options
- Lowest bill of materials and smallest footprint for NFC solution in embedded electronics

3 Applications

NXP NTAG I²C *plus* is a family of connected NFC tags that combine a passive NFC interface with a contact I²C interface. As the second generation of NXP's industry-leading connected-tag technology, these devices maintain full backward compatibility with first-generation NTAG I²C products, while adding new, advanced features for password protection, full memory-access configuration from both interfaces, and an originality signature for protection against cloning.

The second-generation technology provides four times higher pass-through performance, along with energy harvesting capabilities, yet NTAG I²C *plus* devices are optimized for use in NFC applications like:

- IoT nodes (home automation, smart home, etc.)
- Pairing and configuration of consumer applications
- NFC accessories (headsets, speakers, etc.)
- Wearable infotainment
- Fitness equipment
- Consumer electronics
- Healthcare
- Smart printers
- Meters
- Electronic shelf labels

4 Ordering information

Table 1. Ordering information

Type number	Package		
	Name	Description	Version
NT3H2111W0FHK	XQFN8	Plastic, extremely thin quad flat package; no leads; 8 terminals; body 1.6 x 1.6 x 0.5 mm; 1k bytes memory, 50 pF input capacitance	SOT902-3
NT3H2211W0FHK	XQFN8	Plastic, extremely thin quad flat package; no leads; 8 terminals; body 1.6 x 1.6 x 0.5 mm; 2k bytes memory, 50 pF input capacitance	SOT902-3
NT3H2111W0FTT	TSSOP8	Plastic thin shrink small outline package; 8 leads; body width 3 mm; 1k bytes memory; 50 pF input capacitance	SOT505-1
NT3H2211W0FTT	TSSOP8	Plastic thin shrink small outline package; 8 leads; body width 3 mm; 2k bytes memory; 50 pF input capacitance	SOT505-1
NT3H2111W0FT1	SO8	Plastic small outline package; 8 leads; body width 3.9 mm, 1k bytes memory; 50 pF input capacitance	SOT96-1
NT3H2211W0FT1	SO8	Plastic small outline package; 8 leads; body width 3.9 mm, 2k bytes memory; 50 pF input capacitance	SOT96-1
NT3H2111W0FUG	FFC bumped	8 inch wafer, 150um thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 1k Bytes memory, 50 pF input capacitance	-
NT3H2211W0FUG	FFC bumped	8 inch wafer, 150um thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 2k Bytes memory, 50 pF input capacitance	-
REMARK: Wafer specification addendum is available after exchange of a non-disclosure agreement (NDA)			

5 Marking

Table 2. Marking codes

Type number	Marking code		
	Line 1	Line 2	Line 3
NT3H2111W0FHK	211	-	-
NT3H2211W0FHK	221	-	-
NT3H2111W0FTT	32111	DBSN ASID	YWW
NT3H2211W0FTT	32211	DBSN ASID	YWW
NT3H2111W0FT1	NT32111	DBSN ASID	nDYWW
NT3H2211W0FT1	NT32211	DBSN ASID	nDYWW

Used abbreviations:

DBSN: Diffusion Batch Sequence Number

ASID: Assembly Sequence ID

n: Assembly Centre Code

D: RHF-2006 indicator

Y: year

WW: week

6 Block diagram

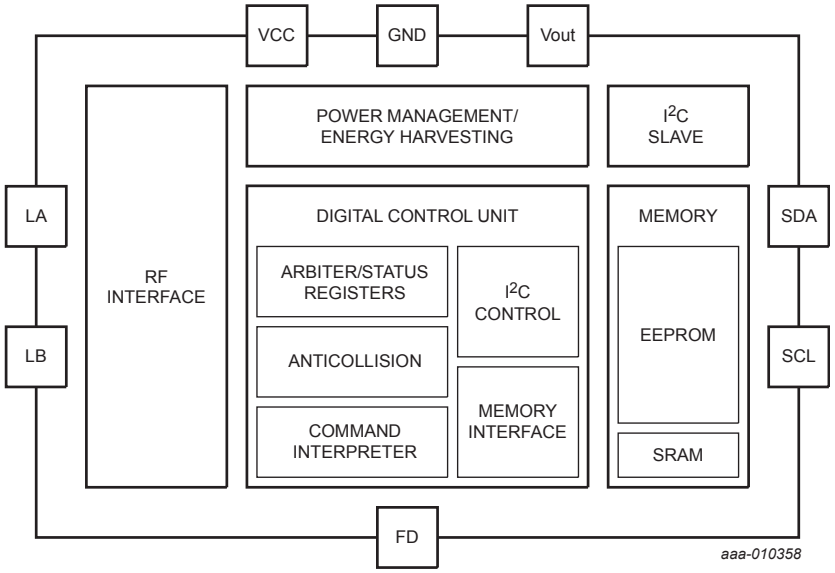


Figure 2. Block diagram

7 Pinning information

7.1 Pinning

7.1.1 XQFN8

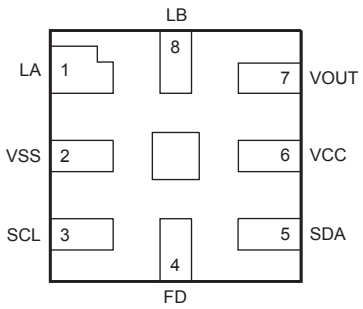


Figure 3. Pin configuration for XQFN8

Detailed package and soldering information may be found in Section 17.

7.1.2 TSSOP8

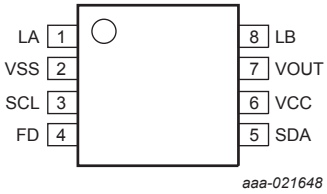


Figure 4. Pin configuration for TSSOP8

Detailed package and soldering information may be found in Section 17.

7.1.3 SO8

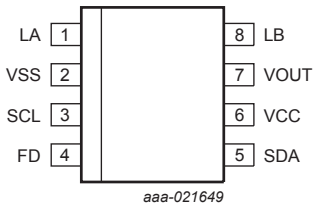


Figure 5. Pin configuration for SO8

Detailed package and soldering information may be found in Section 17.

7.2 Pin description

Table 3. Pin description for XQFN8, TSSOP8 and SO8

Pin	Symbol	Description
1	LA	Antenna connection LA
2	VSS	GND
3	SCL	Serial clock I²C
4	FD	Field detection
5	SDA	Serial data I²C
6	VCC	VCC in connection (external power supply)
7	VOUT	Voltage out (energy harvesting)
8	LB	Antenna connection LB

8 Functional description

8.1 Block description

NTAG I²C *plus* ICs consist of EEPROM, SRAM, NFC interface, Digital Control Unit (Command interpreter, Anticollision, Arbiter/Status registers, I²C control and Memory Interface), Power Management and Energy Harvesting Unit and an I²C slave interface. Energy and data are transferred via an antenna consisting of a coil with a few turns, which is directly connected to NTAG I²C *plus* IC.

8.2 NFC interface

The passive NFC-interface is based on the ISO/IEC 14443-3 Type A standard.

It requires to be supplied by an NFC field (e.g. NFC enabled device) always to be able to receive appropriate commands and send the related responses.

As defined in ISO/IEC 14443-3 Type A for both directions of data communication, there is one start bit (start of communication) at the beginning of each frame. Each byte is transmitted with an odd parity bit at the end. The least significant bit of the byte 0 of the selected block is transmitted first.

For a multi-byte parameter, the least significant byte is always transmitted first. For example, when reading from the memory using the READ command, byte 0 from the addressed block is transmitted first, followed by bytes 1 to byte 3 out of this block. The same sequence continues for the next block and all subsequent blocks.

8.2.1 Data integrity

The following mechanisms are implemented in the contactless communication link between the NFC device and the NTAG I²C *plus* IC to ensure very reliable data transmission:

- 16 bits CRC per block
- Parity bits for each byte
- Bit count checking
- Bit coding to distinguish between "1", "0" and "no information"
- Channel monitoring (protocol sequence and bit stream analysis)

The commands are initiated by the NFC device and controlled by the Digital Control Unit of the NTAG I²C *plus* IC. The command response depends on the state of the IC, and for memory operations, the access conditions valid for the corresponding page.

8.2.2 NFC state machine

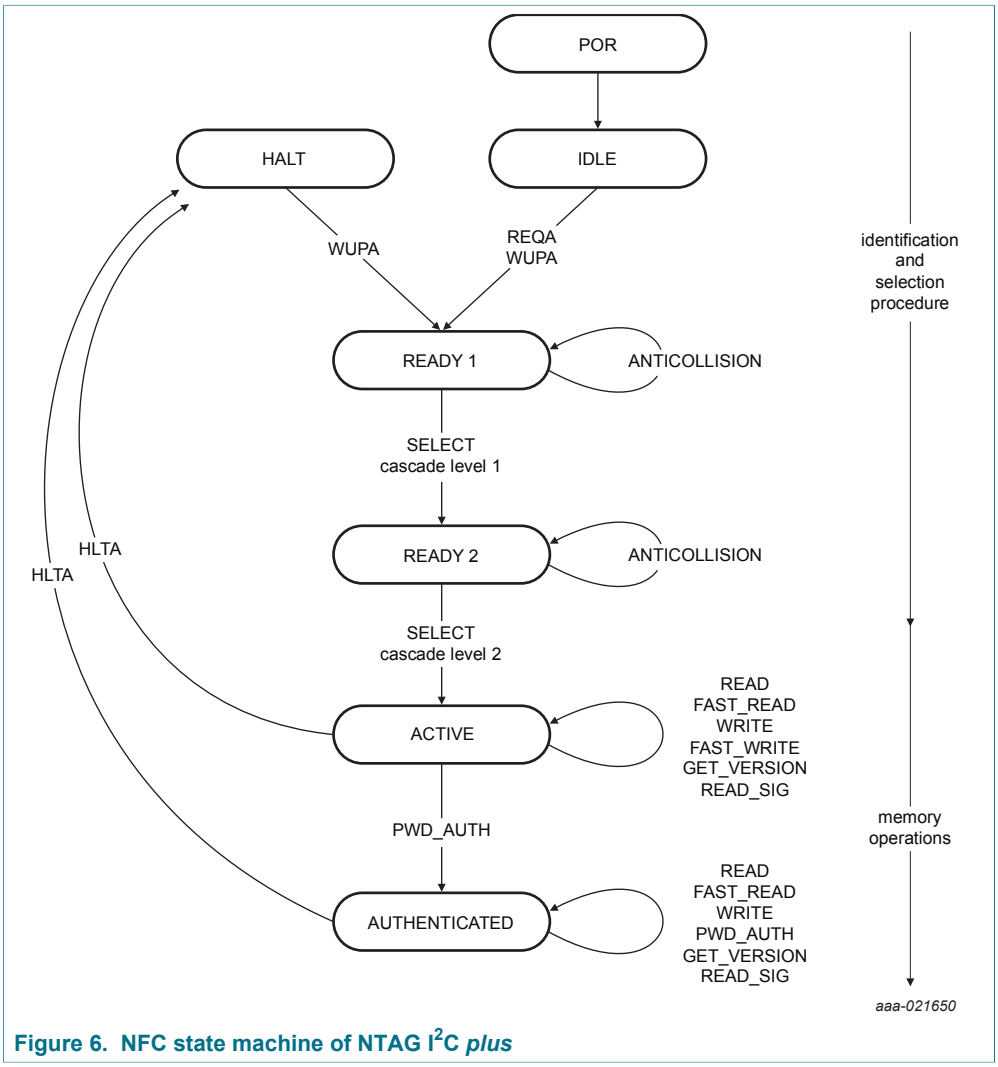


Figure 6. NFC state machine of NTAG I²C *plus*

The overall NFC state machine is summarized in Figure 6. When an error is detected or an unexpected command is received, in each state the tag returns to IDLE or HALT state as defined in ISO/IEC 14443-3 Type A.

8.2.2.1 IDLE state

After a Power-On Reset (POR), the NTAG I²C *plus* switches to the default waiting state, namely the IDLE state. It exits IDLE towards READY 1 state when a REQA or a WUPA command is received from the NFC device. Any other data received while in IDLE state is interpreted as an error, and the NTAG I²C *plus* remains in the IDLE state.

8.2.2.2 READY 1 state

In the READY 1 state, the NFC device resolves the first part of the UID (3 bytes) using the ANTICOLLISION or SELECT commands for cascade level 1. READY 1 state is correctly exited after.

- receiving SELECT command from cascade level 1 with the matching of complete first part of the UID. In this case, the NFC device switches the NTAG I²C *plus* into READY 2 state where the second part of the UID gets resolved.

Remark: The response of the NTAG I²C *plus* to the SELECT command is the Select AcKnowledge (SAK) byte with cascade bit set to 1b indicating that UID is not complete.

8.2.2.3 READY 2 state

In the READY 2 state, the NFC device resolves the second part of the UID (4 bytes) using the ANTICOLLISION or SELECT command for cascade level 2. READY2 state is correctly exited after.

- receiving SELECT command from cascade level 2 with the matching of complete second part of the UID. In this case, the NFC device switches the NTAG I²C *plus* into ACTIVE state where all application-related commands can be executed.

Remark: The response of the NTAG I²C *plus* to the SELECT command in READY 2 state is the Select AcKnowledge (SAK) byte with cascade bit cleared to indicate, that NTAG I²C *plus* is now uniquely selected and only this device will communicate with the NFC device even when other contactless devices are present in the NFC device field.

8.2.2.4 ACTIVE state

All unprotected memory operations are operated in the ACTIVE and AUTHENTICATED states.

The ACTIVE state is exited with the PWD_AUTH command or with the HLTA command.

Upon reception of a correct password within PWD_AUTH command, the NTAG I²C *plus* transits to AUTHENTICATED state after responding with PACK.

With the HLTA command, the NTAG I²C *plus* transits to the HALT state.

Any other invalid command in ACTIVE state is interpreted as an error. Depending on its previous state, the NTAG I²C *plus* returns to either to the IDLE or HALT state.

8.2.2.5 AUTHENTICATED state

Protected memory operations are only operated in the AUTHENTICATED state, however access to the unprotected memory is possible, too.

The AUTHENTICATED state is exited with the HLTA command and upon reception, the NTAG I²C *plus* transits to the HALT state.

Any other invalid command in AUTHENTICATED state is interpreted as an error. Depending on its previous state, the NTAG I²C *plus* returns to either to the IDLE or HALT state.

8.2.2.6 HALT state

HALT and IDLE states constitute the two waiting states implemented in the NTAG I²C *plus*. An already processed NTAG I²C *plus* in ACTIVE or AUTHENTICATED state can be set into the HALT state using the HLTA command. In the anticollision phase, this state helps the NFC device distinguish between processed tags and tags yet to be selected. The NTAG I²C *plus* can only exit HALT state upon execution of the WUPA command. Any other data received when the device is in this state is interpreted as an error, and NTAG I²C *plus* state remains unchanged.

8.3 Memory organization

The memory map is detailed in Table 4 (1k memory) and Table 5 (2k memory) from the NFC interface and in Table 6 (1k memory) and Table 7 (2k memory) from the I²C interface. The SRAM memory is only available and accessible when powered via VCC. Please refer to Section 11 for examples of memory map from the NFC interface with SRAM mapping.

The structure of manufacturing data, static and dynamic lock bytes, capability container and user memory pages are compatible with other NTAG products.

Any memory access which starts at a valid address and extends into an invalid access region will return 00h value for the invalid region.

Bits and bytes mareked as reserved for future use (RFU) SHALL NOT be changed, as it may lead to unintended tag behaviour.

8.3.1 Memory map from NFC perspective

Memory access from the NFC perspective is organized in pages of 4 bytes each. If password protection is not used, complete user memory is unprotected.

Table 4. NTAG I²C *plus* 1k memory organization from the NFC perspective

Sector address	Page address		Byte number within a page				Access cond. ACTIVE state	Access cond. AUTH. state
	Dec.	Hex.	0	1	2	3		
0	0	00h	Serial number (UID)				READ	
	1	01h	Serial number (UID)			Internal	READ	
	2	02h	Internal		Static lock bytes		READ/R&W	
	3	03h	Capability Container (CC)				READ&WRITE	
	4	04h	Unprotected user memory				READ&WRITE	
	...	...						
	AUTH0	AUTH0	Protected user memory				READ[1]	READ&WRITE
	...	...						
	225	E1h						
	226	E2h	Dynamic lock bytes			00h	R&W/READ	
	227	E3h	RFU	RFU	RFU	AUTH0	READ[1]	READ&WRITE
	228	E4h	ACCESS	RFU	RFU	RFU	READ[1]	READ&WRITE
	229	E5h	PWD[2]				READ[1]	READ&WRITE
	230	E6h	PACK[2]		RFU	RFU	READ[1]	READ&WRITE
	231	E7h	PT_I2C	RFU	RFU	RFU	READ[1]	READ&WRITE
	232	E8h	Configuration registers				see 8.3.12	
	233	E9h						
	234	EAh	Invalid access - returns NAK				n.a.	
	235	EBh						
	236	ECh	Session registers				see 8.3.12	
	237	EDh						
	238	EEh	Invalid access - returns NAK				n.a.	
	239	EFh						
	240	F0h	Invalid access - returns NAK				n.a.	
	...	...						
	255	FFh						
1	...	...	Invalid access - returns NAK				n.a.	
2	...	...	Invalid access - returns NAK				n.a.	
3	0	00h	Invalid access - returns NAK				n.a.	
	...	...						
	248	F8h	Mirrored session registers				see 8.3.12	
	249	F9h						

Sector address	Page address		Byte number within a page				Access cond. ACTIVE state	Access cond. AUTH. state
	Dec.	Hex.	0	1	2	3		
	...	...	Invalid access - returns NAK				n.a.	
	255	FFh						

[1] If NFC_PROT bit is set to 1b, NTAG I²C *plus* returns NAK

[2] On reading PWD or PACK, NTAG I²C *plus* always returns 00h for all bytes

Table 5. NTAG I²C *plus* 2k memory organization from the NFC perspective

Sector address	Page address		Byte number within a page				Access cond. ACTIVE state	Access cond. AUTH. state
	Dec.	Hex.	0	1	2	3		
0	0	00h	Serial number (UID)				READ	
	1	01h	Serial number (UID)			Internal	READ	
	2	02h	Internal		Static lock bytes		READ/R&W	
	3	03h	Capability Container (CC)				READ&WRITE	
	4	04h	Unprotected user memory				READ&WRITE	
	...	...						
	AUTH0	AUTH0	Protected user memory				READ[1]	READ&WRITE
	...	...						
	225	E1h						
	226	E2h	Dynamic lock bytes			00h	R&W/READ	
	227	E3h	RFU	RFU	RFU	AUTH0	READ[1]	READ&WRITE
	228	E4h	ACCESS	RFU	RFU	RFU	READ[1]	READ&WRITE
	229	E5h	PWD[2]				READ[1]	READ&WRITE
	230	E6h	PACK[2]		RFU	RFU	READ[1]	READ&WRITE
	231	E7h	PT_I2C	RFU	RFU	RFU	READ[1]	READ&WRITE
	232	E8h	Configuration registers				see 8.3.12	
	233	E9h						
	234	EAh	Invalid access - returns NAK				n.a.	
	235	EBh						
	236	ECh	Session registers				see 8.3.12	
	237	EDh						
	238	EEh	Invalid access - returns NAK				n.a.	
	...	...						
	255	FFh						
1	0	00h	(Un-)protected user memory[3,4]				see protected user memory in Sector 0	
	...	...						
	255	FFh						
2	...	...	Invalid access - returns NAK				n.a.	
3	0	00h	Invalid access - returns NAK				n.a.	
	...	...						
	248	F8h	Mirrored session registers				see 8.3.12	
	249	F9h						

Sector address	Page address		Byte number within a page				Access cond. ACTIVE state	Access cond. AUTH. state
	Dec.	Hex.	0	1	2	3		
	...	...	Invalid access - returns NAK				n.a.	
	255	FFh						

[1] If NFC_PROT bit is set to 1b, NTAG I²C *plus* returns NAK

[2] On reading PWD or PACK, NTAG I²C *plus* always returns 00h for all bytes

[3] If 2K_PROT bit is set to 1b, complete Sector 1 of NTAG I²C *plus* is password protected

[4] If NFC_DIS_SEC1 bit is set to 1b, complete Sector 1 of NTAG I²C *plus* is not accessible from NFC perspective

8.3.2 Memory map from I²C interface

The memory access of NTAG I²C *plus* from the I²C interface is organized in blocks of 16 bytes each.

I²C slave address is stored in most significant 7 bits of byte 0 in block 0. However, when reading block 0, NTAG I²C *plus* always returns 04h for byte 0.

WARNING: When configuring Static lock bytes and Capability container, Address byte gets updated, too. Address byte consists of slave address (coded in most significant 7 bits) and least significant bit set to 0b.

REMARK: For convenience reasons it is recommended to configure Address byte (block 0, byte 0) to 04h.

Table 6. NTAG I²C *plus* 1k memory organization from the I²C perspective

I²C block address		Byte number within a block				Access conditions		
		0	1	2	3	I²C_PROT		
		4	5	6	7			
		8	9	10	11	00b	01b	1xb
Dec.	Hex.	12	13	14	15			
0	00h	Addr.[1]	Serial number (UID)			READ&WRITE		
		Serial number (UID)			Internal			
		Internal		Static lock bytes				
		Capability Container (CC)						
1	01h	Unprotected user memory				READ&WRITE		
...	...							
AUTH0	AUTH0	Protected user memory				READ&WRITE	READ	NAK
...	...							
55	37h							
56	38h	Protected user memory				READ&WRITE	READ	NAK
		Dynamic lock bytes			00h	READ&WRITE		
		RFU	RFU	RFU	AUTH0			
57	39h	ACCESS	RFU	RFU	RFU			
		PWD[2]						
		PACK[2]		RFU	RFU			
		PT_I2C	RFU	RFU	RFU			
58	3Ah	Configuration registers				see 8.3.12		
		00h	00h	00h	00h	READ		
		00h	00h	00h	00h			
59	3Bh	Invalid access - returns NAK				n.a.		
...	...							
247	F7h							
248	F8h	SRAM memory (64 bytes)				READ&WRITE		
...	...							
251	FBh							
...	...	Invalid access - returns NAK				n.a.		
254	FEh	Session registers				see 8.3.12		
		00h	00h	00h	00h	READ		

I²C block address		Byte number within a block				Access conditions I²C_PROT		
		0	1	2	3	00b	01b	1xb
		4	5	6	7			
		8	9	10	11			
Dec.	Hex.	12	13	14	15			
		00h	00h	00h	00h			
255	FFh	Invalid access - returns NAK				n.a.		

[1] The byte 0 of block 0 is always read as 04h (UID0). Writing to block 0 updates the I²C address.

[2] On reading PWD and PACK, NTAG I²C *plus* always returns 00h for all bytes

Table 7. NTAG I²C *plus* 2k memory organization from the I²C perspective

I²C block address		Byte number within a block				Access conditions		
		0	1	2	3	I²C_PROT		
		4	5	6	7			
		8	9	10	11	00b	01b	1xb
Dec.	Hex.	12	13	14	15			
0	00h	Addr.[1]	Serial number (UID)			READ&WRITE		
		Serial number (UID)			Internal			
		Internal		Static lock bytes				
		Capability Container (CC)						
1	01h	Unprotected user memory				READ&WRITE		
...	...							
AUTH0	AUTH0	Protected user memory				READ&WRITE	READ	NAK
...	...							
56	38h	Protected user memory				READ&WRITE	READ	NAK
		Protected user memory						
		Dynamic lock bytes			00h	READ&WRITE		
		RFU	RFU	RFU	AUTH0			
57	39h	ACCESS	RFU	RFU	RFU			
		PWD[2]						
		PACK[2]		RFU	RFU			
		PT_I2C	RFU	RFU	RFU			
58	3Ah	Configuration registers				see 8.3.12		
		00h	00h	00h	00h	READ		
		00h	00h	00h	00h			
...	...	Invalid access - returns NAK				n.a.		
64	40h	(Un-)protected user memory				READ&WRITE	READ	NAK
...	...							
127	7Fh							
...	...	Invalid access - returns NAK				n.a.		
248	F8h	SRAM memory (64 bytes)				READ&WRITE		
...	...							
251	FBh							
...	...	Invalid access - returns NAK				n.a.		

I²C block address		Byte number within a block				Access conditions I²C_PROT		
		0	1	2	3	00b	01b	1xb
		4	5	6	7			
		8	9	10	11			
Dec.	Hex.	12	13	14	15			
254	FEh	Session registers				see 8.3.12		
		00h	00h	00h	00h	READ		
		00h	00h	00h	00h			
255	FFh	Invalid access - returns NAK				n.a.		

[1] The byte 0 of block 0 is always read as 04h (UID0). Writing to block 0 updates the I²C address.

[2] On reading PWD and PACK, NTAG I²C *plus* always returns 00h for all bytes

8.3.3 EEPROM

The EEPROM is a non-volatile memory that stores the 7 byte UID, the memory lock conditions, IC configuration information and the user memory.

Sector 0 memory map looks totally the same for NTAG I²C *plus* 1k and 2k version, the only difference is the dynamic lock bit granularity.

NXP introduced with NTAG I²C *plus* the possibility to split the memory in an open and a password protected area see Section 8.3.11.

8.3.4 SRAM

For frequently changing data, a volatile memory of 64 bytes with unlimited endurance is built in. The 64 bytes are mapped in a similar way as done in the EEPROM, i.e., 64 bytes are seen as 16 pages of 4 bytes from NFC perspective.

The SRAM is only available when the tag is powered via the VCC pin.

The SRAM is located at the end of the memory space and it is always directly accessible by the I²C host (addresses F8h to FBh). An NFC device cannot access the SRAM memory in normal mode (i.e., outside the pass-through mode). The SRAM is only accessible by the NFC device if the SRAM is mirrored onto the EEPROM memory space.

With SRAM mirror enabled (SRAM_MIRROR_ON_OFF = 1b - see Section 11.2), the SRAM can be mirrored in the User Memory from start page 01h to 74h for access from the NFC side.

The Memory mirror must be enabled once both interfaces are ON as this feature is disabled after each POR.

The register SRAM_MIRROR_BLOCK (see Table 14) indicates the address of the first page of the SRAM buffer. In the case where the SRAM mirror is enabled and the READ command is addressing blocks where the SRAM mirror is located, the SRAM byte values will be returned instead of the EEPROM byte values. Similarly, if the tag is not VCC powered, the SRAM mirror is disabled and reading out the bytes related to the SRAM mirror position would return the values from the EEPROM.

In the pass-through mode (PTHRU_ON_OFF = 1b - see Section 8.3.12), the SRAM is mirrored to the fixed address F0h - FFh for NFC access (see Section 11) in the first memory sector (Sector 0) of NTAG I²C *plus*.

8.3.5 Serial number (UID)

The unique 7-byte serial number (UID) is programmed into the first 7 bytes of memory covering page addresses 00h and 01h - see Figure 7. These bytes are programmed and write protected during production.

UID0 is fixed to the value 04h - the manufacturer ID for NXP Semiconductors in accordance with ISO/IEC 14443-3.

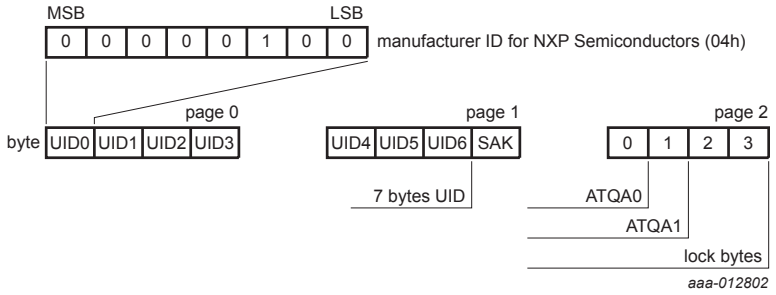


Figure 7. Serial number (UID)

8.3.6 Static Lock Bytes

According to NFC Forum Type 2 Tag specification, the bits of byte 2 and byte 3 of page 02h (via NFC) or byte 10 and 11 address 00h (via I²C) represent the field programmable, read-only locking mechanism (see Figure 8). Each page from 03h (CC) to 0Fh can be individually locked by setting the corresponding locking bit to logic 1b to prevent further write access. After locking, the corresponding page becomes read-only memory.

This read only locking is address-based. This means, when SRAM is mirrored to these blocks, also SRAM blocks are read only from NFC prespective.

In addition, NTAG I²C *plus* uses the three least significant bits of lock byte 0 as the block-locking bits. Bit 2 controls pages 0Ah to 0Fh (via NFC), bit 1 controls pages 04h to 09h (via NFC) and bit 0 controls page 03h (CC). Once the block-locking bits are set, the locking configuration for the corresponding memory area is frozen, e.g. cannot be changed to read-only anymore.

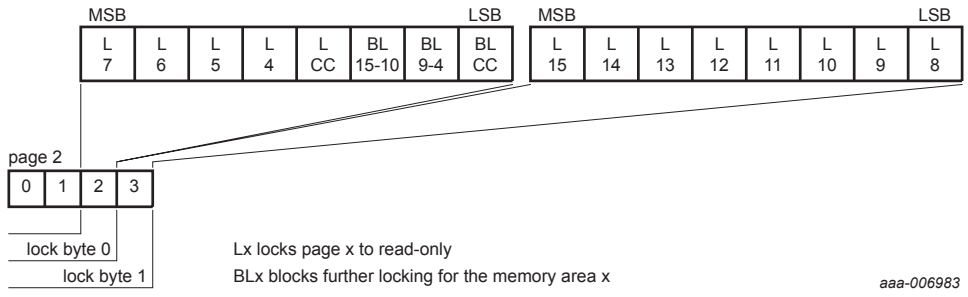


Figure 8. Static lock bytes 0 and 1

For example, if BL15-10 is set to logic 1b, then bits L15 to L10 (lock byte 1, bit[7:2]) can no longer be changed. The static locking and block-locking bits are set by the bytes 2 and 3 of the WRITE command to page 02h. The contents of the lock bytes are bit-wise OR'ed and the result then becomes the new content of the lock bytes. This process is irreversible from NFC perspective. If a bit is set to logic 1b, it cannot be changed back to logic 0b. From I²C perspective, the bits can be reset to 0b by writing bytes 10 and 11 of block 00h. As I²C address is coded in byte 0 of block 0, it may be changed unintentionally.

The contents of bytes 0 and 1 of page 02h (via NFC) are unaffected by the corresponding data bytes of the WRITE command.

The default value of the static lock bytes is 0000h.

8.3.7 Dynamic Lock Bytes

To lock the pages of NTAG I²C *plus* starting at page address 16 and onwards, the dynamic lock bytes are used. The dynamic lock bytes are located in Sector 0 at page E2h. The three lock bytes cover the memory area of 840 data bytes (NTAG I²C *plus* 1k) or 1864 data bytes (NTAG I²C *plus* 2k). The granularity is 16 pages for NTAG I²C *plus* 1k (see Figure 9) and 32 pages for NTAG I²C *plus* 2k (see Figure 10) compared to a single page for the first 48 bytes (see Figure 8).

NTAG I²C *plus* needs a Lock Control TLV as specified in NFC Forum Type 2 Tag specification to ensure NFC Forum Type 2 Tag compliancy.

When NFC Forum Type 2 Tag transition to READ ONLY state is intended, all bits marked as RFUI and dynamic lock bits related to the protected area shall be set to 0b when writing to the dynamic lock bytes.

The default value of the dynamic lock bytes is 000000h. The value of Byte 3 is always 00h when read.

Like for the static lock bytes, this process of modifying the dynamic lock bits is irreversible from NFC perspective and applies also for potentially mirrored SRAM. If a bit is set to logic 1b, it cannot be changed back to logic 0b. From I²C interface, these bits can be set to 0b again.

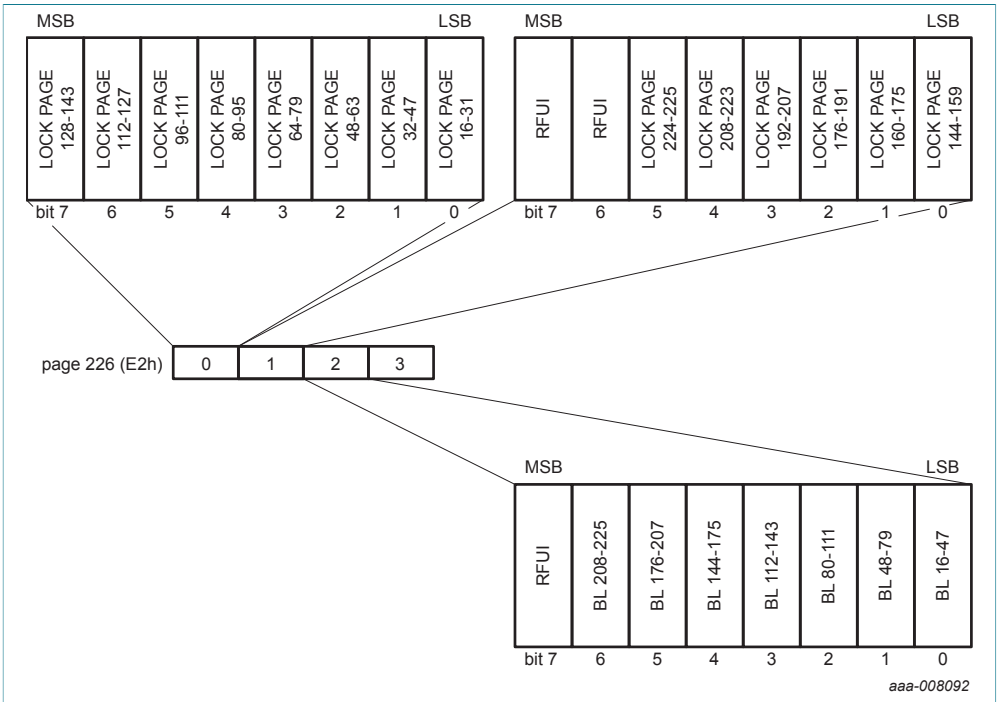


Figure 9. NTAG I²C *plus* 1k Dynamic lock bytes 0, 1 and 2

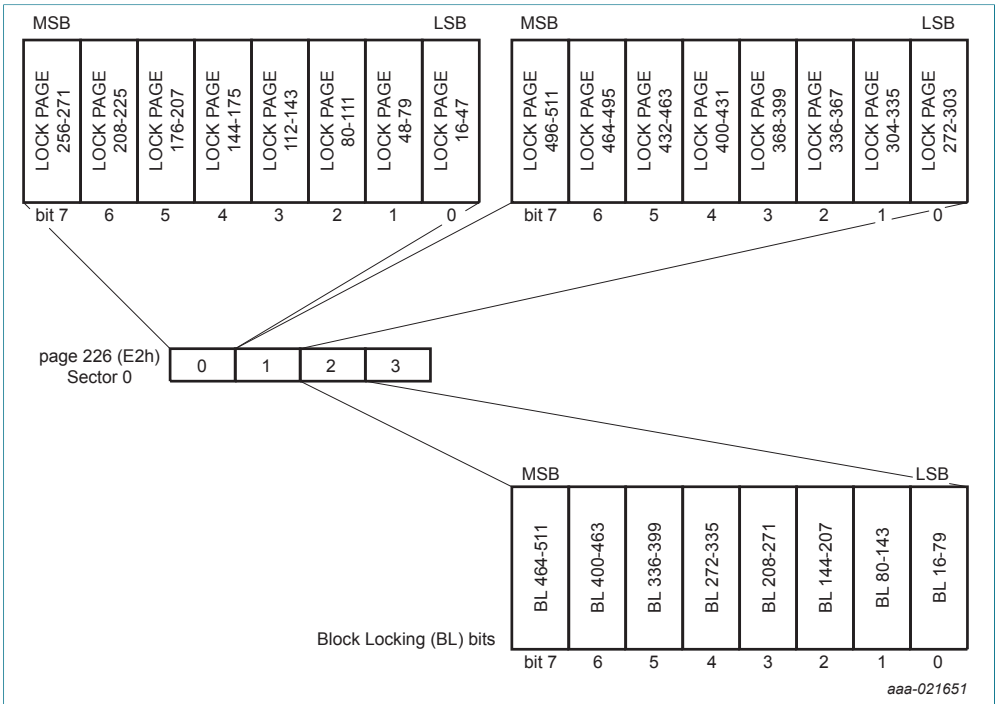


Figure 10. NTAG I²C *plus* 2k Dynamic lock bytes 0, 1 and 2

8.3.8 Capability Container (CC)

According to NFC Forum Type 2 Tag specification the CC is located on page 03h (see Ref. 1). To keep full flexibility to split the memory into an open and protected area, the default value of the CC is initialized with 00000000h during the IC production.

NDEF messages can only be written with NFC Forum devices, after setting these CC bytes according to application-specific needs and NFC Forum specification by a WRITE command from the I²C or NFC interface. According to NFC Forum specification, a bit once set to 1b, an NFC Forum Device cannot set bits of the CC back to 0b. However, similar to the lock bits, setting these bits back to 0b is again possible from I²C perspective.

WARNING: As I²C address (byte 0) and static lock bytes (byte 10 and byte 11) are coded in block 00h from I²C side, the I²C address may be changed or the tag may be locked unintentionally, when changing CC.

REMARK: When reading out byte 0, NTAG I²C *plus* always returns 04h (UID0). Therefore, for convenience reasons it is recommended to configure I²C address byte to 04h.

NXP recommends setting the size parameter of the CC only to values that the T2T_Area ends at lock bit granularity boundaries when using only part of the memory for storing NDEF messages. Consequently T2T_Area size should be 112 + 64*N or 888 bytes with N less or equal to 13 for the 1k version, or 176 + 128*N or 2032 bytes with N less or equal to 14 for the 2k version.

In Figure 11 it is shown how the CC is changed when going from READ/WRITE to READ ONLY state according to NFC Forum.

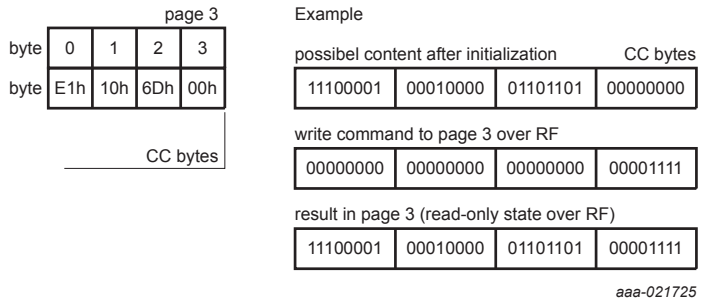


Figure 11. Possible configuration of CC bytes of NTAG I²C 1k version

8.3.9 User Memory pages

Pages 04h to E1h of Sector 0 via the NFC interface - Block 01h to 37h, plus the first 8 bytes of block 38h via the I²C interface is the user memory area for NTAG I²C *plus* 1k and 2k version.

In addition, complete Sector 1 (page 00h to FFh) via the NFC interface - block 40h to 7Fh via the I²C interface is used as user memory area for NTAG I²C *plus* 2k version.

8.3.10 Memory content at delivery

As described above the CC in page 03h is set to all 00h to keep the full flexibility. To allow NFC Forum NDEF message reading and writing page 03h (CC) and the following data page (NDEF TLV) of NTAG I²C *plus* need to be initialized by the user according to

the NFC Forum Type 2 Tag specification (see Ref. 1). Table 8 shows an example of NFC Forum-compliant content using the whole memory of sector 0 for NDEF messages.

Remark: The default content of the data pages from page 04h onwards is not defined at delivery.

Table 8. Minimum memory content to be in initialized state for NTAG I²C *plus*

Page Address	Byte number within page			
	0	1	2	3
03h	E1h	10h	6Dh	00h
04h	03h	00h	FEh	00h

8.3.11 Password and Access Configuration

NTAG I²C *plus* can be configured to have password protected memory areas.

If this feature is used, NXP recommends changing and diversify the PWD and PACK for every single chip.

The password and access configuration area of pages E3h to E7h (Sector 0 - see Table 9) via the NFC interface or blocks 38h and 39h via the I²C interface are used to configure the password and access conditions of the NTAG I²C *plus*. Those bit values are stored in the EEPROM. Their values can be read and written by both interfaces when applicable and when not locked by the register lock bits (see REG_LOCK in Table 13).

AUTH0 defines the starting page address of the protected area in Sector 0. NXP recommends setting AUTH0 in a way always respecting the lock bit granularity. Setting AUTH0 greater EBh, disables password protection.

The NFC_PROT bit is used to either only require a PWD_AUTH for writing data to the protected area or even protect reading data from the protected area.

If password authentication is used, even the SRAM access can be protected by setting SRAM_PROT bit to 1b.

I2C_PROT enables the possibility to limit access to the protected area from I²C perspective to read only or no access at all.

AUTLIM value can be used to limit negative PWD_AUTH attempts.

For the 2k version of NTAG I²C *plus* NFC_DIS_SEC1 bit can be used to disable the access to Sector 1 from NFC perspective with the 2K_PROT bit password protection for Sector 1 can be enabled.

Once password protection is enabled, writing to Password and Access Configuration bytes is only possible after a successful password authentication. On reading the PWD or PACK, from NFC or I²C perspective, NTAG I²C *plus* always returns all 00h bytes.

A detailed description of the mechanism and how to program all the parameters is given in Section 8.7.

Table 9. Password and Access Configuration Register

NFC page address (Sector 0)		I²C block address		Byte number from NFC perspective			
Dec	Hex	Dec	Hex	0	1	2	3
224	E0h	56	38h	User Memory			
225	E1h						
226	E2h			Dynamic lock bytes			00h
227	E3h			RFU	RFU	RFU	AUTH0
228	E4h	57	39h	ACCESS	RFU	RFU	RFU
229	E5h			PWD			
230	E6h			PACK		RFU	RFU
231	E7h			PT_I2C	RFU	RFU	RFU

Table 10. Password and Access Configuration bytes

Bit	Field	Access via NFC	Access via I²C	Default values	Description
Authentication Pointer (AUTH0)					
7-0	AUTH0	R&W	R&W	FFh	Page address of Sector 0 from which onwards the password authentication is required to access the user memory from NFC perspective, dependent on NFC_PROT bit. If AUTH0 is set to a page address greater than EBh, the password protection is effectively disabled. Password protected area starts from page AUTH0 and ends at page EBh. Password protection is excluded for Dynamic Lock Bits, session registers and mirrored SRAM pages. **REMARK:** From I²C interface, you have access to all configuration pages until REG_LOCK_I2C bit is set to 1b.
Access Conditions (ACCESS)					
7	NFC_PROT	R&W	R&W	0b	Memory protection bit: 0b: write access to protected area is protected by the password 1b: read and write access to protected area is protected by the password
6	RFU	R&W	R&W	0b	RFU - SHALL be 0b
5	NFC_DIS_SEC1	R&W	R&W	0b	NFC access protection to Sector 1 0b: Sector 1 is accessible in 2k version 1b: Sector 1 in inaccessible and returns NAK0
4-3	RFU	R&W	R&W	00b	RFU - SHALL be 00b

Bit	Field	Access via NFC	Access via I²C	Default values	Description
2-0	AUTHLIM	R&W	R&W	000b	Limitation of negative password authentication attempts. After reaching the limit, protected area is not accessible any longer. 000b: limiting of negative password authentication attempts disabled. 001b-111b: maximum number of negative password authentication attempts is $2^{AUTHLIM}$
Password (PWD)					
31-0	PWD	R&W	R&W	FFFFFFFFh	32-bit password used for memory access protection. Reading PWD always returns 00000000h
Password Acknowledge (PACK)					
15-0	PACK	R&W	R&W	0000h	16-bit password acknowledge used during the password authentication process. Reading PACK always returns 0000h
Protection bits (PT_I2C)					
7-4	RFU	R&W	R&W	0000b	RFU - SHALL be 0000b
3	2K_PROT	R&W	R&W	0b	Password protection for Sector 1 for 2k version 0b: password authentication for Sector 1 disabled 1b: password authentication needed to access Sector 1
2	SRAM_PROT	R&W	R&W	0b	Password protection for pass-through and mirror mode 0b: password authentication for pass-through mode disabled 1b: password authentication needed to access SRAM in pass-through mode
1-0	I2C_PROT	R&W	R&W	00b	Access to protected area from I²C perspective 00b: Entire user memory accessible from I²C 01b: read and write access to unprotected user area, read only access to protected area 1Xb: read and write access to unprotected area, no access to protected area. **REMARK:** Independent from these bits I²C always has R&W access to: • Session registers • SRAM • Configuration pages including PWD Configuration area, but dependent on REG_LOCK_I2C bit

8.3.12 NTAG I²C configuration and session registers

NTAG I²C *plus* behavior can be configured and read in two separate locations depending if the configurations shall be effective within the communication session (use session registers) or by default after Power-On Reset (POR) (use configuration registers).

The configuration registers of pages E8h to E9h (Sector 0 - see Table 11) via the NFC interface or block 3Ah via the I²C interface are used to configure the default behavior of the NTAG I²C *plus*. Those bit values are stored in the EEPROM and represent the

default settings to be effective after POR. Their values can be read and written by both interfaces when applicable and when not locked by the register lock bits (see REG_LOCK in Table 13).

Table 11. Configuration register NTAG I²C *plus*

NFC address (Sector 0)		I²C Address		Byte number from NFC perspective			
Dec	Hex	Dec	Hex	0	1	2	3
232	E8h	58	3Ah	NC_REG	LAST_NDEF_BLOCK	SRAM_MIRROR_BLOCK	WDT_LS
233	E9h			WDT_MS	I2C_CLOCK_STR	REG_LOCK	RFU

The session register on pages ECh to EDh (Sector 0) via the NFC interface or block FEh via I²C, see Table 12, are used to configure or monitor the values of the current communication session. Those bits are read only via the NFC interface but may be read and written via the I²C interface.

For backward compatibility reasons the session registers are mirrored to Sector 3 (page F8h and F9h via the NFC interface).

Table 12. Session registers NTAG I²C *plus*

NFC address (Sector 0)		I²C Address		Byte number			
Dec	Hex	Dec	Hex	0	1	2	3
236	ECh	254	FEh	NC_REG	LAST_NDEF_BLOCK	SRAM_MIRROR _BLOCK	WDT_LS
237	EDh			WDT_MS	I2C_CLOCK_STR	NS_REG	RFU

Both, the session and the configuration registers have the same configuration options and parameters except the REG_LOCK bits, which are only available in the configuration register and the NS_REG bits which are only available in the session register. After POR, the content of the configuration register is loaded into the session register.

The values of both registers can be changed during a communication session. If the desired effect should be visible immediately, but only for the current communication session, the session registers must be used. After POR, the session registers values will again contain the configuration register values as before.

To change the default behavior, changes to the configuration register are needed, but the related effect will only be visible after the next POR.

To make the effect immediately and after next POR visible, changes to configuration and session registers are needed.

All registers and configuration default values, access conditions and descriptions are defined in Table 13 and Table 14.

Reading and writing the session registers via I²C can only be done via the READ and WRITE registers operation - see Section 9.8.

Table 13. Configuration bytes

Bit	Field	Access via NFC	Access via I²C	Default values	Description
Configuration register: NC_REG					
7	NFCS_I2C_RST_ON_OFF	R&W	R&W	0b	Enables the NFC silence feature and enables soft reset through I²C repeated start - see Section 9.3
6	PTHRU_ON_OFF	R&W	R&W	0b	1b: pass-through mode using SRAM enabled and SRAM mapped to end of Sector 0. 0b: pass-through mode disabled
5-4	FD_OFF	R&W	R&W	00b	defines the event upon which the signal output on the FD pin is released 00b: if the field is switched off 01b: if the field is switched off or the tag is set to the HALT state 10b: if the field is switched off or the last page of the NDEF message has been read (defined in LAST_ NDEF_BLOCK) 11b: (if FD_ON = 11b) if the field is switched off or if last data is read by I²C (in pass-through mode NFC ---> I²C) or last data is written by I²C (in pass-through mode I²C---> NFC) 11b: (if FD_ON = 00b or 01b or 10b) if the field is switched off See Section 8.4 for more details
3-2	FD_ON	R&W	R&W	00b	defines the event upon which the signal output on the FD pin is pulled low 00b: if the field is switched on 01b: by first valid start of communication (SoC) 10b: by selection of the tag 11b: (in pass-through mode NFC-->I²C) if the data is ready to be read from the I²C interface 11b: (in pass-through mode I²C--> NFC) if the data is read by the NFC interface See Section 8.4 for more details
1	SRAM_MIRROR_ON_OFF	R&W	R&W	0b	1b: SRAM mirror enabled and mirrored SRAM starts at page SRAM_MIRROR_BLOCK 0b: SRAM mirror disabled
0	TRANSFER_DIR	R&W	R&W	1b	defines the data flow direction when pass-through mode is enabled 0b: from I²C to NFC interface 1b: from NFC to I²C interface In case the pass-through mode is NOT enabled, this bit should be set to 1b, otherwise there is no WRITE access from the NFC perspective
Configuration register: LAST_NDEF_BLOCK					

Bit	Field	Access via NFC	Access via I²C	Default values	Description
7-0	LAST_NDEF_BLOCK	R&W	R&W	00h	I²C block address of I²C block, which contains last byte(s) of stored NDEF message. An NFC read of the last page of this I²C block sets the register NDEF_DATA_READ to 1b and triggers field detection pin if FD_OFF is set to 10b. Valid range starts from 01h (NFC page 04h) up to 37h (NFC page DCh) for NTAG I²C *plus* 1k or up to 7Fh (NFC page FCh on Sector 1) for NTAG I²C *plus* 2k.
Configuration register: SRAM_MIRROR_BLOCK					
7-0	SRAM_MIRROR_BLOCK	R&W	R&W	F8h	I²C block address of SRAM when mirrored into the User memory. Valid range starts from 01h (NFC page 04h) up to 34h (NFC page D0h) for NTAG I²C *plus* 1k or up to 7Ch (NFC page F0h on memory Sector 1) for NTAG I²C *plus* 2k
Configuration register: WDT_LS					
7-0	WDT_LS	R&W	R&W	48h	Least Significant byte of watchdog time control register
Configuration register: WDT_MS					
7-0	WDT_MS	R&W	R&W	08h	Most Significant byte of watchdog time control register. When writing WDT_MS byte, the content of WDT_MS and WDT_LS gets active for the watchdog timer.
Configuration register: I2C_CLOCK_STR					
7-1	RFU	R&W	R&W	0000000b	RFU - all 7 bits SHALL be 0b
0	I2C_CLOCK_STR	R&W	R&W	1b	Enables (1b) or disable (0b) the I²C clock stretching
Configuration register: REG_LOCK					
7-2	RFU	R&W	R&W	000000b	RFU - all 6 bits SHALL be 0b
1	REG_LOCK_I2C[1]	R&W	R&W	0b	I²C Configuration Lock Bit 0b: Configuration bytes may be changed via I²C 1b: Configuration bytes cannot be changed via I²C Once set to 1b, cannot be reset to 0b anymore.
0	REG_LOCK_NFC[1]	R&W	R&W	0b	NFC Configuration Lock Bit 0b: Configuration bytes may be changed via NFC 1b… Configuration bytes cannot be changed via NFC Once set to 1b, cannot be reset to 0b anymore.

[1] Setting both bits REG_LOCK_I2C and REG_LOCK_NFC to 1b, permanently locks write access to register default values (as no write is allowed anymore). As long as one bit is still 0b, the corresponding interface can still access and change the register lock bytes.

Table 14. Session register bytes

Bit	Field	Access via NFC	Access via I²C	Default values	Description
Session register: NC_REG					
7	NFCS_I2C_RST_ON_OFF	READ	R&W	-	see configuration bytes description
6	PTHRU_ON_OFF	READ	R&W	-	see configuration bytes description, the bit is cleared automatically, when one of the interfaces is OFF
5-4	FD_OFF	READ	R&W	-	see configuration bytes description
3-2	FD_ON	READ	R&W		
1	SRAM_MIRROR_ON_OFF	READ	R&W	-	see configuration bytes description, the bit is cleared automatically, when there is no Vcc power.
0	TRANSFER_DIR	READ	R&W		see configuration bytes description
Session register: LAST_NDEF_BLOCK					
7-0	LAST_NDEF_BLOCK	READ	R&W	-	see configuration bytes description
Session register: SRAM_MIRROR_BLOCK					
7-0	SRAM_MIRROR_BLOCK	READ	R&W	-	see configuration bytes description
Session register: WDT_LS					
7-0	WDT_LS	READ	R&W	-	see configuration bytes description
Session register: WDT_MS					
7-0	WDT_MS	READ	R&W	-	see configuration bytes description
Session register: I2C_CLOCK_STR					
7-2	RFU	READ	READ	-	RFU, all 6 bits locked to 0b
1	NEG_AUTH_REACHED	READ	READ	0b	Status bit to show the number of negative PWD_AUTH attempts reached 0b: PWD_AUTH still possible 1b: PWD_AUTH locked
0	I2C_CLOCK_STR	READ	READ	-	See configuration bytes description
Session register: NS_REG					
7	NDEF_DATA_READ	READ	READ	0b	1b: all data bytes read from the address specified in LAST_NDEF_BLOCK. Bit is reset to 0b when read
6	I2C_LOCKED	READ	R&W	0b	1b: Memory access is locked to the I²C interface
5	RF_LOCKED	READ	READ	0b	1b: Memory access is locked to the NFC interface
4	SRAM_I2C_READY	READ	READ	0b	1b: data is ready in SRAM buffer to be read by I2C
3	SRAM_RF_READY	READ	READ	0b	1b: data is ready in SRAM buffer to be read by NFC
2	EEPROM_WR_ERR	READ	R&W	0b	1b: HV voltage error during EEPROM write or erase cycle Needs to be written back via I²C to 0b to be cleared

Bit	Field	Access via NFC	Access via I²C	Default values	Description
1	EEPROM_WR_BUSY	READ	READ	0b	1b: EEPROM write cycle in progress - access to EEPROM disabled 0b: EEPROM access possible
0	RF_FIELD_PRESENT	READ	READ	0b	1b: NFC field is detected

8.4 Configurable Field Detection Pin

The field detection pin based on open-drain implementation provides the capability to trigger an external device (e.g. µController) or switch on the connected circuitry by an external power management unit depending on activities on the NFC interface.

As the field detection pin functionality is operated via NFC field power, V_{CC} supply for the tag itself is not required.

NOTE: In some cases V_{OUT} pin might be used as field detection trigger.

The conditions for pulling the field detection signal to low, FD_ON can be:

- The presence of the NFC field
- The detection of a valid command (Start of Communication)
- The selection of the IC

REMARK: When FD_ON is configured to trigger on NFC field presence (00b), FD will be pulled low again, when host is reading the NDEF_DATA_READ bit of NS_REG session register from I²C perspective.

The conditions for releasing the field detection signal defined with FD_OFF can be:

- The absence of the NFC field
- The detection of the HALT state
- The NFC interface has read the last part of the NDEF message defined with LAST_NDEF_BLOCK

All the various combinations of configurations are described in Table 13 and illustrated in Figure 13, Figure 14 and Figure 15 for all various combinations of the filed detection signal configuration. The timing diagrams are not in scale and all given timing values are typical values.

The field detection pin can be used also as a handshake mechanism in the pass-through mode to signal to the external µController if

- New data is written to SRAM on the NFC interface
- Data written to SRAM from the µController is read via the NFC interface.

See Section 11 for more information on this handshake mechanism.

In Figure 12 an example how to connect the FD pin is given. All given values are typical values and may vary from application to application.

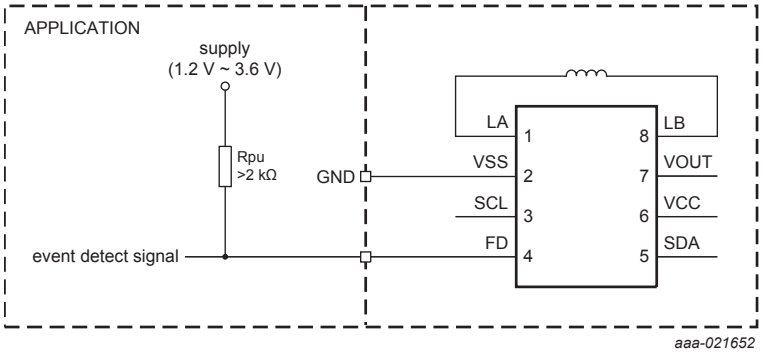


Figure 12. FD pin example circuit

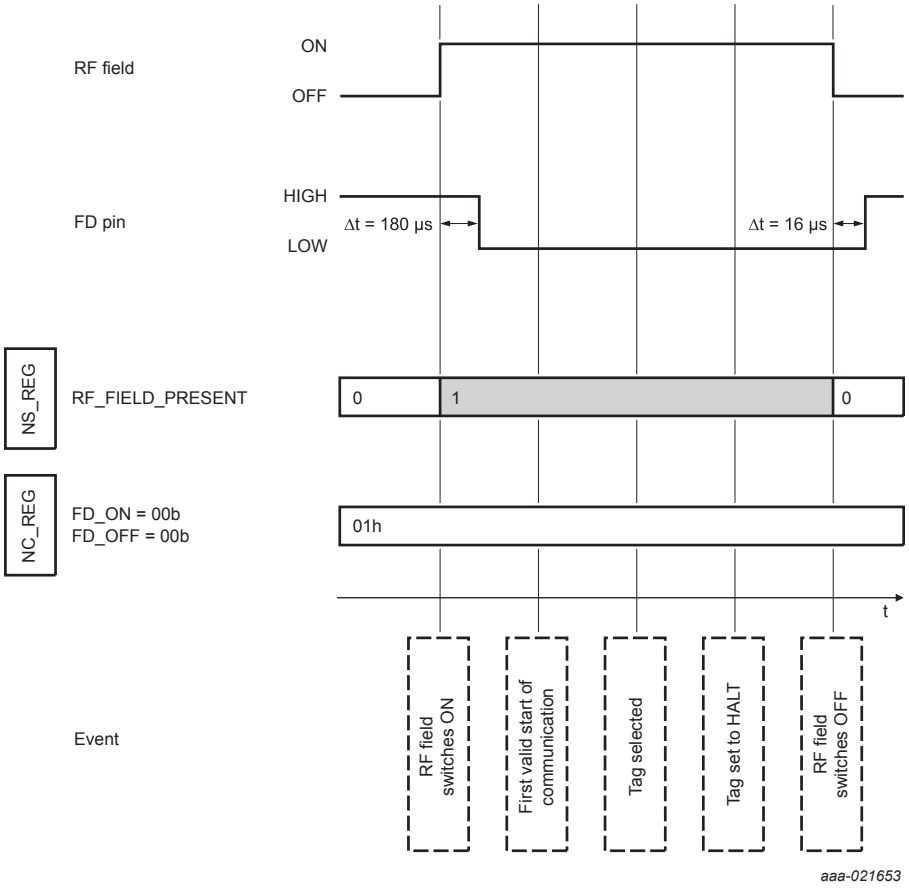


Figure 13. Illustration of the field detection feature when configured for simple field detection

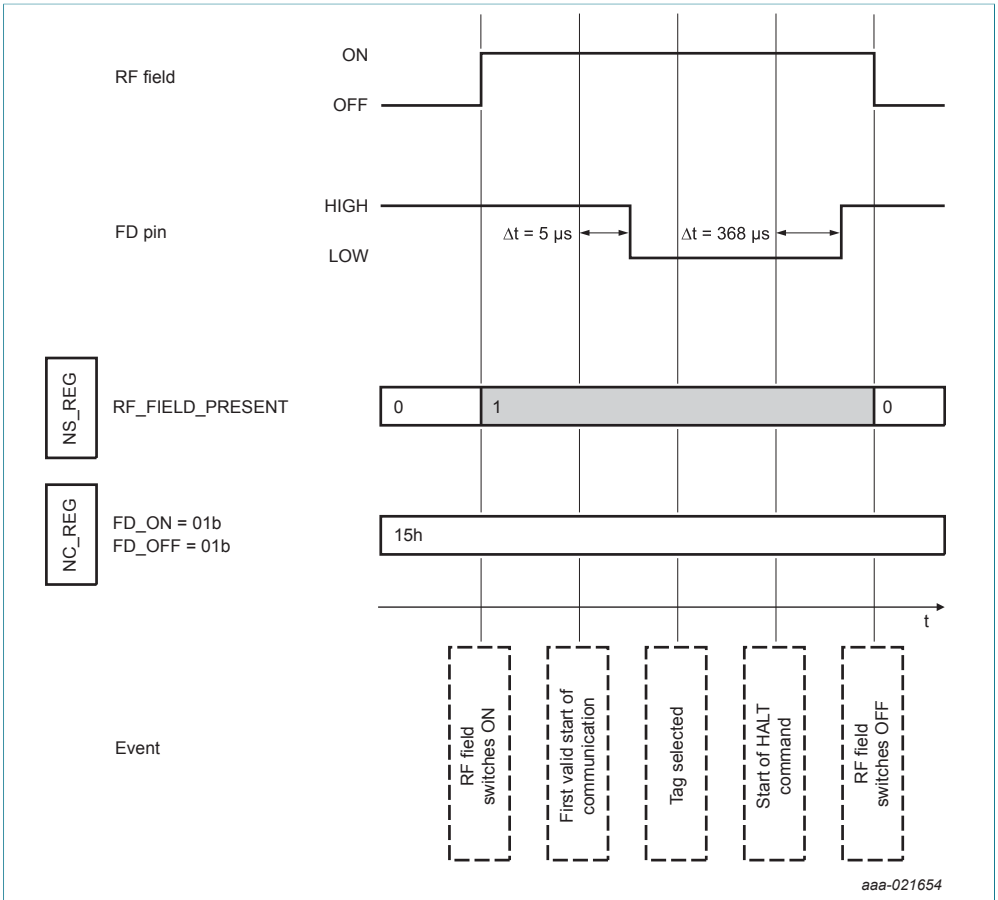


Figure 14. Illustration of the field detection feature when configured for first valid start of communication detection

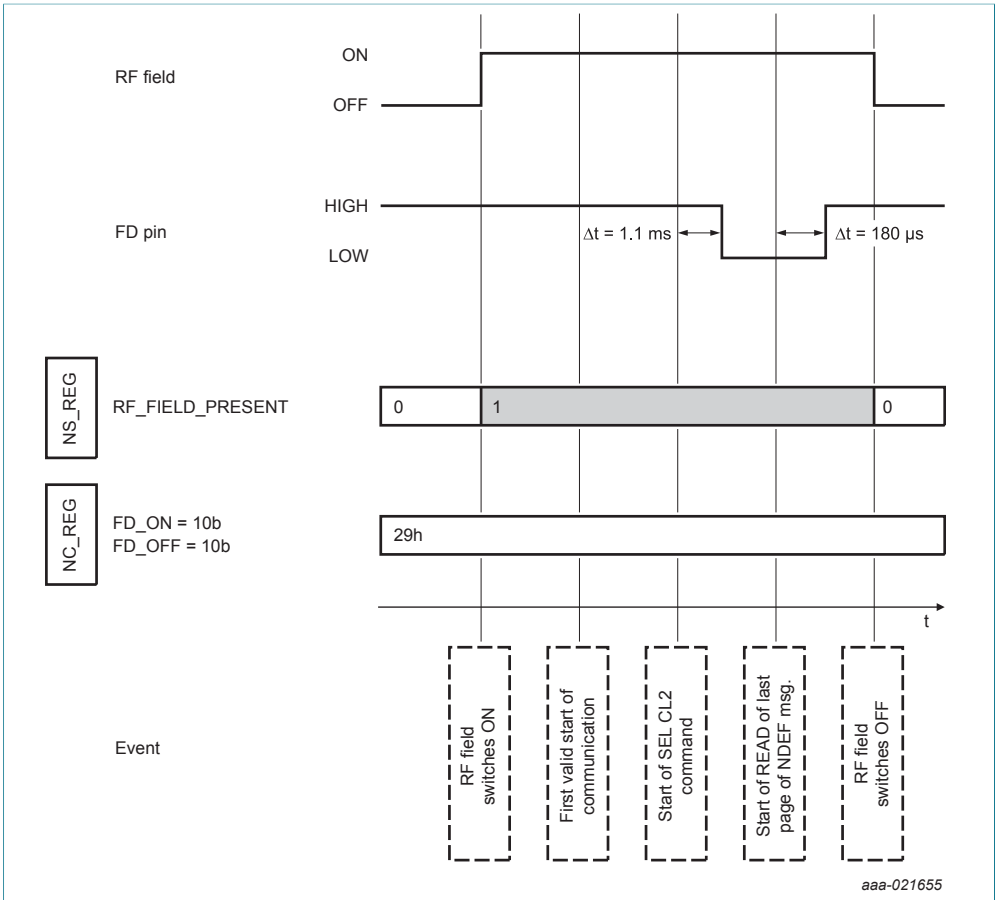


Figure 15. Illustration of the field detection feature when configured for selection of the tag detection

8.5 Watchdog timer

In order to allow the I²C interface to perform all necessary commands (READ, WRITE, ..), the memory access remains locked to the I²C interface until the register I2C_LOCKED is cleared by the host - see Table 14.

However, to avoid that the memory stays 'locked' to the I²C for a long period of time, it is possible to program a watchdog timer to unlock the I²C host from the tag, so that the NFC device can access the tag after a period of time of inactivity. The host itself will not be notified of this event directly, but the NS_REG register is updated accordingly (the register bit I2C_LOCKED will be cleared - see Table 14).

The default value is set to 20 ms (848h), but the watch dog timer can be freely set from 0001h (9.43 µs) up to FFFFh (617.995 ms). The timer starts ticking when the communication between the NTAG I²C and the I²C interface starts. In case the communication with the I²C is still going on after the watchdog timer expires, the communication will continue until the communication has completed. Then the status register I2C_LOCKED will be immediately cleared.

In the case where the communication with the I²C interface has completed before the end of the timer and the status register I2C_LOCKED was not cleared by the host, it will be cleared at the end of the watchdog timer.

The watchdog timer is only effective if the VCC pin is powered and will be reset and stopped if the NTAG I²C is not VCC powered or if the register status I2C_LOCKED is set to 0 and RF_LOCKED is set to 1b.

8.6 Energy harvesting

The NTAG I²C *plus* provides the capability to supply external low-power devices with energy harvested from the NFC field of an NFC device as illustrated in Figure 16. All given values are typical values. For more details, refer to Ref. 7.

The voltage and current from the energy harvesting depend on various parameters, such as the strength of the NFC field, the tag antenna size, or the distance from the NFC device. NTAG I²C *plus* provides typically 5 mA at 2 V on the VOUT pin with an NFC Phone.

Operating NTAG I²C in energy harvesting mode requires a number of precautions:

- A complete total connected capacitor in the range of typically 150 nF up to 220 nF maximum shall be connected between VOUT and GND close to the terminals to ensure that the voltage does not drop below VCC min during modulation or during any application operation.
- Start up load current on VOUT should be limited until sufficient voltage is built on VOUT.
- If NTAG I²C also powers the I²C bus, then VCC must be connected to VOUT, and pull-up resistors on the SCL and SDA pins must be sized to control SCL and SDA sink current when those lines are pulled low by NTAG I²C or the I²C host
- If NTAG I²C also powers the Field Detect bus, then the pull-up resistor on the Field Detect line must be sized to control the sink current into the Field Detect pin when NTAG I²C pulls it low
- The NFC reader device communicating with NTAG I²C shall apply polling cycles including an NFC Field Off condition of at least 5.1 ms as defined in NFC Forum Activity specification (see Ref. 4, chapter 6).

REMARK: increasing the output current on V_{out} decreases the NFC communication range.

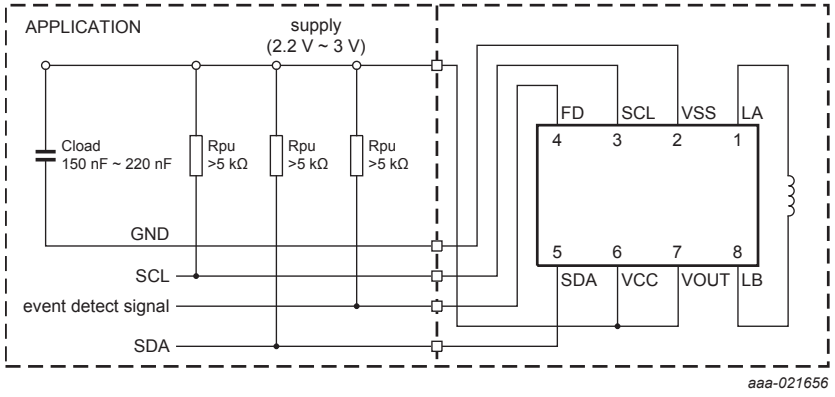


Figure 16. Energy harvesting example circuit

8.7 Password authentication

The memory write or read/write access to a configurable part of the memory can be constrained to a positive password authentication. The 32-bit secret password (PWD) and the 16-bit password acknowledge (PACK) response shall be typically programmed into the configuration pages at the tag personalization stage.

The AUTHLIM parameter specified in Section 8.3.11 can be used to limit the negative authentication attempts.

In the initial state of NTAG I²C *plus*, password protection is disabled by an AUTH0 value of FFh. PWD and PACK are freely writable in this state. Access to the configuration pages and any part of the user memory can be restricted by setting AUTH0 to a page address within the available memory space. This page address is the first one protected.

For a comprehensive description of all protection mechanism refer to Ref. 9.

Remark: The password protection method provided in NTAG I²C *plus* has to be intended as an easy and convenient way to prevent unauthorized memory accesses. If a higher level of protection is required, cryptographic methods can be implemented at application layer to increase overall system security.

8.7.1 Programming of PWD and PACK

The 32-bit PWD and the 16-bit PACK need to be programmed into the configuration pages, see Section 8.3.11. The password as well as the password acknowledge are written LSByte first. This byte order is the same as the byte order used during the PWD_AUTH command and its response.

The PWD and PACK bytes can never be read out of the memory. Instead of transmitting the real value on any valid read command from both - NFC and I²C - interface, only 00h bytes are replied.

If the password authentication is disabled, PWD and PACK can be written at any time.

If the password authentication is enabled, PWD and PACK can be written after a successful PWD_AUTH command only.

Remark: To improve the overall system security, it is advisable to diversify the password and the password acknowledge using a die individual parameter of the IC, which can be the 7-byte UID available on NTAG I²C *plus*.

8.7.2 Limiting negative verification attempts

To prevent brute-force attacks on the password, the maximum allowed number of negative password authentication attempts can be set using AUTHLIM. This mechanism is disabled by setting AUTHLIM to a value of 000b, which is also the initial state of NTAG I²C *plus*.

If AUTHLIM is not equal to 000b, each negative authentication verification is internally counted. As soon as this internal counter reaches the number $2^{AUTHLIM}$, any further negative password authentication leads to a permanent locking of the protected part of the memory for the specified access modes. Independently, whether the provided password is correct or not, each subsequent PWD_AUTH fails.

Any successful password verification, before reaching the limit of negative password verification attempts, resets the internal counter to zero.

8.7.3 Protection of configuration segments

The configuration pages can be protected by the password authentication as well. The protection level is defined with the NFC_PROT bit.

The protection is enabled by setting the AUTH0 byte (see Table 10) to a value that is within the addressable memory space.

8.8 Originality signature

NTAG I²C *plus* features a cryptographically supported originality check. With this feature, it is possible to verify that the tag is using an IC manufactured by NXP Semiconductors. This check can be performed on personalized tags as well.

NTAG I²C *plus* digital signature is based on standard Elliptic Curve Cryptography (ECC), according to the ECDSA algorithm. The use of a standard algorithm and curve ensures easy software integration of the originality check procedure in an application running on an NFC device without specific hardware requirements.

Each NTAG I²C *plus* UID is signed with an NXP private key and the resulting 32-byte signature is stored in a hidden part of the NTAG I²C *plus* memory during IC production.

This signature can be retrieved using the READ_SIG command and can be verified in the NFC device by using the corresponding ECC public key provided by NXP. In case the NXP public key is stored in the NFC device, the complete signature verification procedure can be performed offline.

To verify the signature (for example with the use of the public domain crypto library OpenSSL) the tool domain parameters shall be set to secp128r1, defined within the standards for elliptic curve cryptography SEC (Ref. 10).

Details on how to check the signature value are provided in corresponding application note (Ref. 6). It is foreseen to offer not only offline, as well as online way to verify originality of NTAG I²C *plus*.

9 I²C commands

For details about I²C interface refer to Ref. 3.

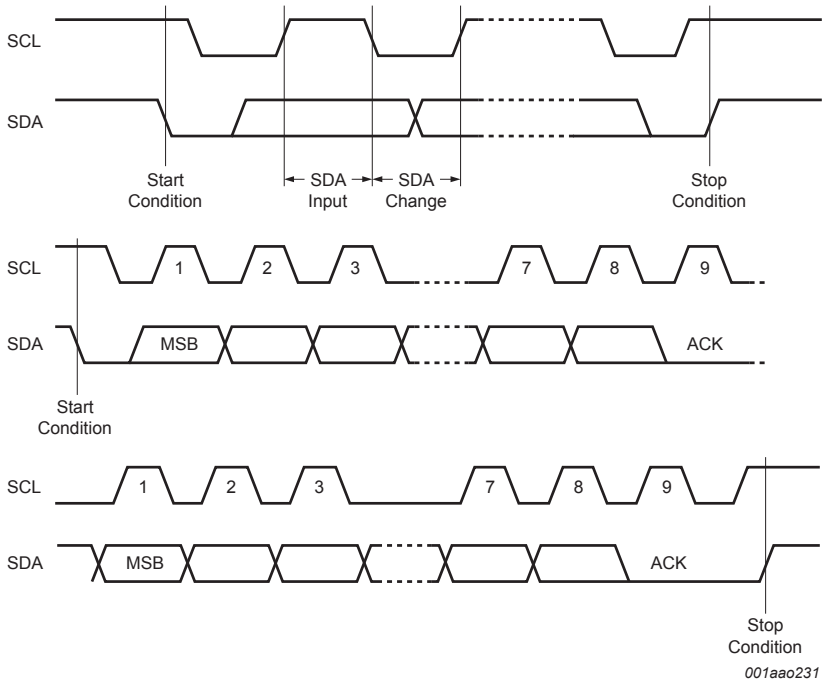


Figure 17. I²C bus protocol

The NTAG I²C *plus* supports the I²C protocol. This protocol is summarized in Figure 17. Any device that sends data onto the bus is defined as a transmitter, and any device that reads the data from the bus is defined as a receiver. The device that controls the data transfer is known as the "bus master", and the other as the "slave" device. A data transfer can only be initiated by the bus master, which will also provide the serial clock for synchronization. The NTAG I²C *plus* is always a slave in all communications.

9.1 Start condition

Start is identified by a falling edge of Serial Data (SDA), while Serial Clock (SCL) is stable in the high state. A Start condition must precede any data transfer command. The NTAG I²C *plus* continuously monitors SDA (except during a Write cycle) and SCL for a Start condition, and will not respond unless one is given.

9.2 Stop condition

Stop is identified by a rising edge of SDA while SCL is stable and driven high. A Stop condition terminates communication between the NTAG I²C *plus* and the bus master. A Stop condition at the end of a Write command triggers the internal Write cycle.

WARNING: Host shall respect EEPROM programming time (~4 ms) after this Stop condition in any case. If host sends next command too early, the memory may be corrupted as ongoing EEPROM write cycle might get terminated.

9.3 I²C soft reset and NFC silence feature

With the bit NFCS_I2C_RST_ON_OFF (see Table 13) NTAG I²C *plus* enables two features: a soft reset of the I²C subsystem, and NFC silence, in which the NFC demodulator is disabled.

The I²C soft reset feature interprets an I²C repeated start (no I²C stop in between) as a command to execute a soft reset of the I²C subsystem. This is useful when heavy bus interference can cause the I²C interface to get stuck. A drawback of this feature is that every start symbol then has to be terminated with a Stop, slowing down communication. If a Stop is forgotten, the I²C interface is cleared and previous communication, if any, is lost. Consequently when this feature is used, stop conditions after MEMA for READ/WRITE (see Figure 18) and after REGA for READ/WRITE registers (see Figure 19) shall be send.

The NFC silence feature disables the demodulator. When feature is set, no NFC commands are received, and no replies are issued to commands that were not fully received when NFC Silence was set. This feature allows the tag to "disappear" even if it still is in the reader field. NTAG I²C *plus* will remain in the ISO state it was in when NFC silence was enabled, until NFC silence is removed.

The combination of these two features in a single bit means that I²C soft reset is only active during NFC silence.

9.4 Acknowledge bit (ACK)

The acknowledge bit is used to indicate a successful byte transfer. The bus transmitter, whether it is the bus master or slave device, releases Serial Data (SDA) after sending eight bits of data. During the ninth clock pulse period, the receiver pulls Serial Data (SDA) low to acknowledge the receipt of the ninth data bits.

9.5 Data input

During data input, the NTAG I²C *plus* samples SDA on the rising edge of SCL. For correct device operation, SDA must be stable during the rising edge of SCL, and the SDA signal must change only when SCL is driven low.

9.6 Addressing

To start communication between a bus master and the NTAG I²C *plus* slave device, the bus master must initiate a Start condition (see Section 9.1). Following this initiation, the bus master sends the 7-bit device address, called Slave Address (SA) in following figures.

The 8th bit is the Read/Write bit (R/$\overline{W}$). This bit is set to 1b for Read and 0b for Write operations.

Default device address of 55h results in AAh default I²C write address and ABh default I²C read address.

As from I²C perspective I²C address can be configured via byte 0 of block 0. Reading this block gives 04h, as it is returning UID0 (see Section 8.3.2). Therefore it is recommended to us 04h as I²C write address (02h device address).

NOTE: Byte 0 of block 0 is used to configure the device address. The 7-bit device address needs to be programmed in the 7 most significant bits of this byte. Least

significant bit needs to be set to 0b when programming the device address. E.g. to keep default device address of 55h, byte 0 of block 0 needs to be set to AAh.

If a match occurs on the device address, the NTAG I²C *plus* gives an acknowledgment on SDA during the 9th bit time. If the NTAG I²C *plus* address does not match, it deselects itself from the bus and clears the register I2C_LOCKED (see Table 12).

Table 15. Default NTAG I²C address from I²C

	Device / Slave Address (SA)							R/$\overline{W}$
	b7	b6	b5	b4	b3	b2	b1	b0
Value[1]	1	0	1	0	1	0	1	1/0

[1] Initial values can be changed from I²C perspective

The I²C address of the NTAG I²C *plus* (byte 0 - block 0h) can only be modified by the I²C interface. Both interfaces cannot read the device address and a READ command from the NFC or I²C interface to this byte will return 04h (UID 0 - manufacturer ID for NXP Semiconductors - see Figure 7).

9.7 READ and WRITE Operation

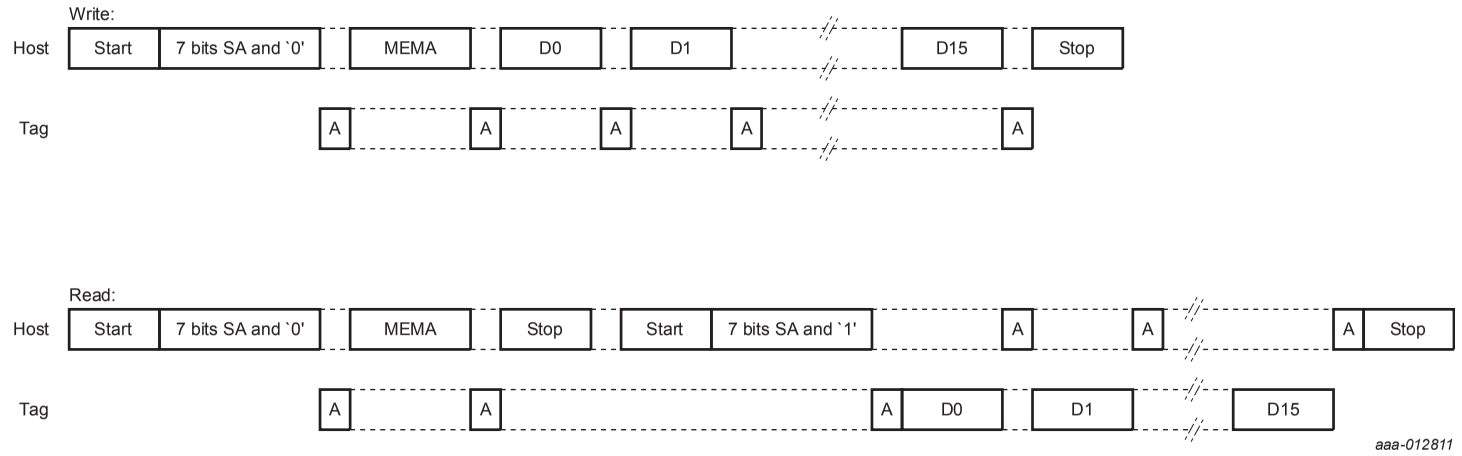


Figure 18. I²C READ and WRITE operation

The READ and WRITE operation always handle 16 bytes to be read or written (one block - see Table 6)

For the READ operation (see Figure 18), following a Start condition, the bus master/host sends the NTAG I²C slave address code (SA - 7 bits) with the Read/Write bit (R/$\overline{W}$) set to 0b. The NTAG I²C *plus* acknowledges this (A), and waits for one address byte (MEMA), which should correspond to the address of the block of memory (SRAM or EEPROM) that is intended to be read. The NTAG I²C *plus* responds to a valid address byte with an acknowledge (A). A Stop condition can be then issued. Then the host again issues a start condition followed by the NTAG I²C *plus* slave address with the Read/Write bit set to 1b. When I2C_CLOCK_STR is set to 0b, a pause of at least 50 µs shall be kept before this start condition. The NTAG I²C *plus* acknowledges this (A) and sends the first byte of data read (D0).The bus master/host acknowledges it (A) and the NTAG I²C *plus* will subsequently transmit the following 15 bytes of memory read with an acknowledge from the host after every byte. After the last byte of memory data has been transmitted by the NTAG I²C *plus*, the bus master/host will acknowledge it and issue a Stop condition.

WARNING: READ sequence shall be atomic. Complete sequence of above figure needs to be executed, otherwise that tag may go to undefined state and stretches the clock infinitely.

For the WRITE operation (see Figure 18), following a Start condition, the bus master/host sends the NTAG I²C *plus* slave address code (SA - 7 bits) with the Read/Write bit (R/$\overline{W}$) set to 0b. The NTAG I²C *plus* acknowledges this (A), and waits for one address byte (MEMA), which should correspond to the address of the block of memory (SRAM or EEPROM) that is intended to be written. The NTAG I²C *plus* responds to a valid address byte with an acknowledge (A) and, in the case of a WRITE operation, the bus master/host starts transmitting every 16 bytes (D0...D15) that shall be written at the specified address with an acknowledge of the NTAG I²C *plus* after each byte (A). After the last byte acknowledge from the NTAG I²C *plus*, the bus master/host issues a Stop condition.

WARNING: Host shall respect EEPROM programming time (~4 ms) after this Stop condition in any case. If host sends next command too early, the memory may be corrupted as ongoing EEPROM write cycle will get terminated.

The memory address accessible via the READ and WRITE operations can only correspond to the EEPROM or SRAM (respectively 00h to 3Ah or F8h to FBh for NTAG I²C *plus* 1k and 00h to 7Ah or F8h to FBh for NTAG I²C *plus* 2k).

9.8 WRITE and READ register operation

In order to modify or read the session register bytes (see Table 14), NTAG I²C *plus* requires the WRITE and READ register operation (see Figure 19).

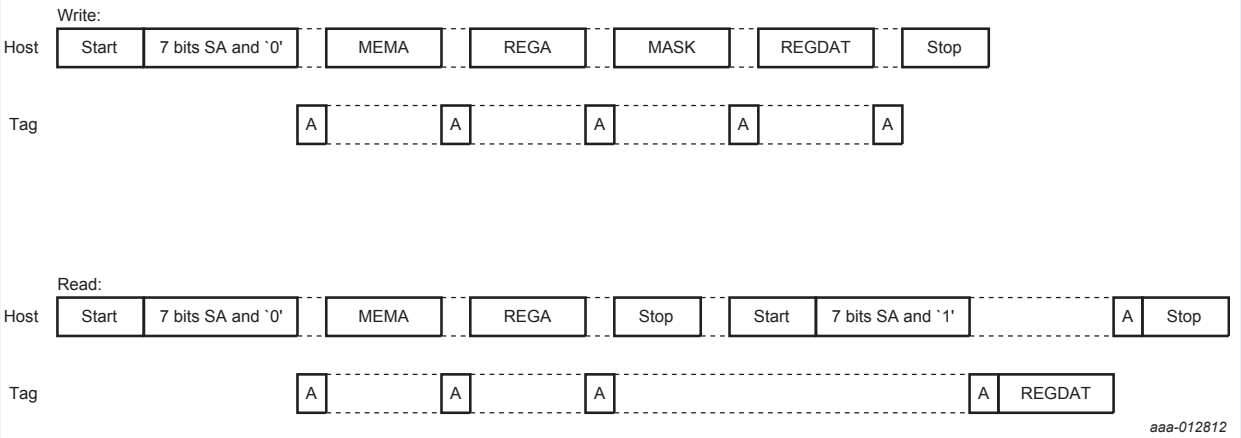


Figure 19. WRITE and READ register operation

For the READ register operation, following a Start condition the bus master/host sends the NTAG I²C *plus* slave address code (SA - 7 bits) with the Read/Write bit (R/$\overline{W}$) set to 0b. The NTAG I²C *plus* acknowledges this (A), and waits for one address byte (MEMA) which corresponds to the address of the block of memory with the session register bytes (FEh). The NTAG I²C *plus* responds to the address byte with an acknowledge (A). Then the bus master/host issues a register address (REGA), which corresponds to the address of the targeted byte inside the block FEh (00h, 01h...to 07h) and then waits for the Stop condition.

Then the bus master/host again issues a start condition followed by the NTAG I²C *plus* slave address with the Read/Write bit set to 1b. The NTAG I²C *plus* acknowledges this (A), and sends the selected byte of session register data (REGDAT) within the block FEh. The bus master/host will acknowledge it and issue a Stop condition.

WARNING: READ sequence shall be atomic. Complete sequence of above figure needs to be executed, otherwise that tag may go to undefined state and stretches the clock infinitely.

For the WRITE register operation, following a Start condition, the bus master/host sends the NTAG I²C *plus* slave address code (SA - 7 bits) with the Read/Write bit (R/$\overline{W}$) set to 0b. The NTAG I²C *plus* acknowledges this (A), and waits for one address byte (MEMA), which corresponds to the address of the block of memory within the session register bytes (FEh). After the NTAG I²C *plus* acknowledge (A), the bus master/host issues a register address (REGA), which corresponds to the address of the targeted byte inside the block FEh (00h, 01h...to 07h). After acknowledgement (A) by NTAG I²C *plus*, the bus master/host issues a MASK byte that defines exactly which bits shall be modified by a 1b bit value at the corresponding bit position. Following the NTAG I²C *plus* acknowledge (A), the new register data (one byte - REGDAT) to be written is transmitted by the bus master/host. The NTAG I²C *plus* acknowledges it (A), and the bus master/host issues a stop condition.

10 NFC Command

NTAG activation follows the ISO/IEC 14443-3 Type A specification. After NTAG I²C *plus* has been selected, it can either be deactivated using the ISO/IEC 14443 HALT command, or NTAG commands (e.g. READ_SIG, PWD_AUTH, SECTOR_SELECT, READ or WRITE) can be performed. For more details about the card activation refer to Ref. 2.

10.1 NTAG I²C *plus* command overview

All available commands for NTAG I²C *plus* are shown in Table 16.

Table 16. Command overview

Command[1]	ISO/IEC 14443	NFC FORUM	Command code (hexadecimal)
Request	REQA	SENS_REQ	26h (7 bit)
Wake-up	WUPA	ALL_REQ	52h (7 bit)
Anticollision CL1	Anticollision CL1	SDD_REQ CL1	93h 20h
Select CL1	Select CL1	SEL_REQ CL1	93h 70h
Anticollision CL2	Anticollision CL2	SDD_REQ CL2	95h 20h
Select CL2	Select CL2	SEL_REQ CL2	95h 70h
Halt	HLTA	SLP_REQ	50h 00h
GET_VERSION	-	-	60h
READ	-	READ	30h
FAST_READ	-	-	3Ah
WRITE	-	WRITE	A2h
FAST_WRITE	-	-	A6h
SECTOR_SELECT	-	SECTOR_SELECT	C2h
PWD_AUTH	-	-	1Bh
READ_SIG	-	-	3Ch

[1] Unless otherwise specified, all commands use the coding and framing as described in Ref. 1.

10.2 Timing

The command and response timing shown in this document are not to scale and values are rounded to 1 µs.

All given command and response times refer to the data frames, including start of communication and end of communication. They do not include the encoding (like the Miller pulses). An NFC device data frame contains the start of communication (1 "start bit") and the end of communication (one logic 0 + 1-bit length of unmodulated carrier). An NFC tag data frame contains the start of communication (1 "start bit") and the end of communication (1-bit length of no subcarrier).

The minimum and maximum command response time is specified according to Ref. 1. The minimum frame delay time from NFC tag to NFC device is 86.43 µs. The maximum command response time is specified as a timeout value. Depending on the command,

the T_{ACK} value specified for command responses defines the NFC device to NFC tag frame delay time. It does it for either the 4-bit ACK value specified or for a data frame.

All timing can be measured according to the ISO/IEC 14443-3 frame specification as shown for the Frame Delay Time in Figure 20. For more details, refer to Ref. 2.

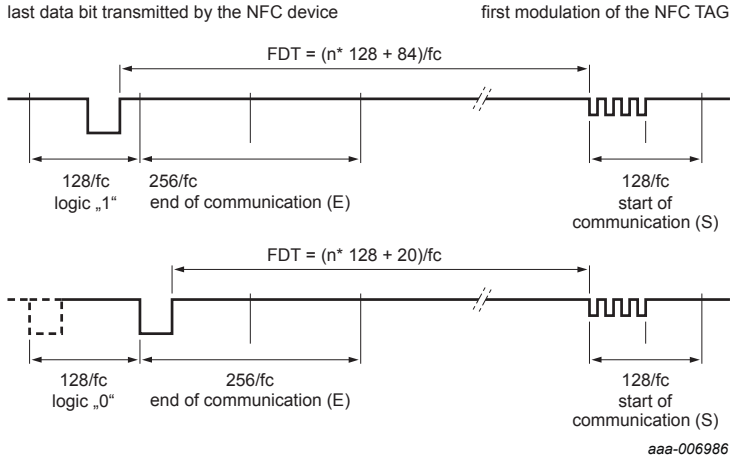


Figure 20. Frame Delay Time (from NFC device to NFC tag), T_{ACK} and T_{NAK}

Remark: Due to the coding of commands, the measured timings usually exclude (a part of) the end of communication. Consider this factor when comparing the specified with the measured times.

10.3 NTAG ACK and NAK

NTAG I²C *plus* uses a 4-bit ACK / NAK as shown in Table 17.

Table 17. ACK and NAK values

Code (4 bit)	ACK/NAK
Ah	Acknowledge (ACK)
0h	NAK for invalid argument (i.e. invalid page address or wrong password)
1h	NAK for parity or CRC error
3h	NAK for Arbiter locked to I²C
4h	Number of negative PWD_AUTH commands limit reached
7h	NAK for EEPROM write error

10.4 ATQA and SAK responses

NTAG I²C *plus* replies to a REQA or WUPA command with the ATQA value shown in Table 18. It replies to a Select CL2 command with the SAK value shown in Table 19. The 2-byte ATQA value is transmitted with the least significant byte first (44h).

Table 18. ATQA response of the NTAG I²C *plus*

		Bit number															
Sales type	**Hex value**	**15**	**14**	**13**	**12**	**11**	**10**	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
NTAG I²C *plus*	00 44h	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0

Table 19. SAK response of the NTAG I²C *plus*

		Bit number							
Sales type	**Hex value**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
NTAG I²C *plus*	00h	0	0	0	0	0	0	0	0

Remark: The ATQA coding in bits 7 and 6 indicates the UID size according to ISO/IEC 14443.

Remark: The bit numbering in ISO/IEC 14443 specification starts with bit 1 as least significant bit.

10.5 GET_VERSION

The GET_VERSION command is used to retrieve information about the NTAG family, the product version, storage size and other product data required to identify the specific NTAG I²C *plus*.

This command is also available on other NTAG products to have a common way of identifying products across platforms and evolution steps.

The GET_VERSION command has no arguments and returns the version information for the specific NTAG I²C *plus* type. The command structure is shown in Figure 21 and Table 20.

Table 21 shows the required timing.

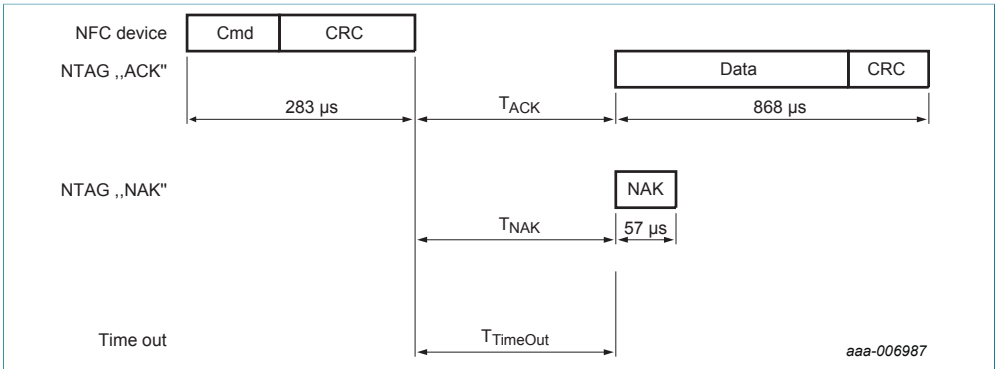


Figure 21. GET_VERSION command

Table 20. GET_VERSION command

Name	Code	Description	Length
Cmd	60h	Get product version	1 byte
CRC	-	CRC according to Ref. 1	2 bytes

Name	Code	Description	Length
Data	-	Product version information	8 bytes
NAK	see Table 17	see Section 10.3	4 bit

Table 21. GET_VERSION timing

These times exclude the end of communication of the NFC device.

	$T_{ACK/NAK}$ min	$T_{ACK/NAK}$ max	$T_{TimeOut}$
GET_VERSION	n=9[1]	$T_{TimeOut}$	5 ms

[1] Refer to Section 10.2 "Timing".

Table 22. GET_VERSION response for NTAG I²C *plus*

Byte no.	Description	NTAG I²C *plus* 1k	NTAG I²C *plus* 2k	Interpretation
0	fixed Header	00h	00h	
1	vendor ID	04h	04h	NXP Semiconductors
2	product type	04h	04h	NTAG
3	product subtype	05h	05h	50 pF I²C, Field detection
4	major product version	02h	02h	2
5	minor product version	02h	02h	V2
6	storage size	13h	15h	see following information
7	protocol type	03h	03h	ISO/IEC 14443-3 compliant

The most significant 7 bits of the storage size byte are interpreted as an unsigned integer value n. As a result, it codes the total available user memory size as 2^n. If the least significant bit is 0b, the user memory size is exactly 2^n. If the least significant bit is 1b, the user memory size is between 2^n and 2^{n+1}.

10.6 READ_SIG

The READ_SIG command returns an IC specific, 32-byte ECC signature, to verify NXP Semiconductors as the silicon vendor. The signature is programmed at chip production and cannot be changed afterwards. The command structure is shown in Figure 24 and Table 27.

Table 28 shows the required timing.

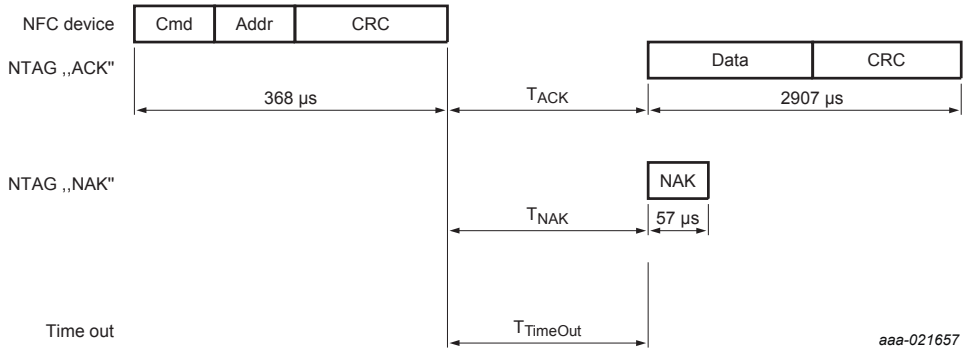


Figure 22. READ_SIG command

Table 23. READ_SIG command

Name	Code	Description	Length
Cmd	3Ch	read ECC signature	1 byte
Addr	00h	RFU, is set to 00h	1 byte
CRC	-	CRC according to Ref. 1	2 bytes
Signature	-	ECC Signature	32 bytes
NAK	see Table 17	see Section 10.3	4 bit

Table 24. READ_SIG timing

These times exclude the end of communication of the NFC device.

	$T_{ACK/NAK}$ min	$T_{ACK/NAK}$ max	$T_{TimeOut}$
READ_SIG	n=9[1]	$T_{TimeOut}$	5 ms

[1] Refer to Section 10.2 "Timing".

Details on how to check the signature value are provided in the corresponding Application note. It is foreseen to offer an online and offline way to verify originality of NTAG I²C *plus*.

10.7 PWD_AUTH

A protected memory area can be accessed only after a successful password verification using the PWD_AUTH command. The AUTH0 configuration byte defines the start of the protected area. It specifies the first page that the password mechanism protects. The level of protection can be configured using the NFC_PROT bit either for write protection or read/write protection. The PWD_AUTH command takes the password as parameter and, if successful, returns the password authentication acknowledge, PACK. By setting the AUTHLIM configuration bits to a value larger than 000b, the number of unsuccessful password verifications can be limited. Each unsuccessful authentication is then counted. After reaching the limit ($2^{AUTHLIM}$) of unsuccessful attempts, the memory write access or the memory access at all (specified in NFC_PROT) to the protected area, is no longer possible. The PWD_AUTH command is shown in Figure 23 and Table 25.

Table 26 shows the required timing.

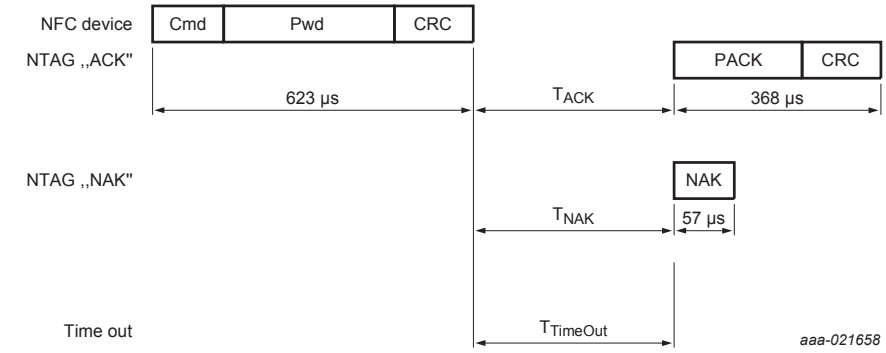


Figure 23. PWD_AUTH command

Table 25. PWD_AUTH command

Name	Code	Description	Length
Cmd	1Bh	password authentication	1 byte
Pwd	-	password	4 bytes
CRC	-	CRC according to Ref. 2	2 bytes
PACK	-	password authentication acknowledge	2 bytes
NAK	see Table 17	see Section 10.3	4-bit

Table 26. PWD_AUTH timing

These times exclude the end of communication of the NFC device.

	$T_{ACK/NAK}$ min	$T_{ACK/NAK}$ max	$T_{TimeOut}$
PWD_AUTH	n=9[1]	$T_{TimeOut}$	5 ms

[1] Refer to Section 10.2 "Timing".

Remark: It is strongly recommended to change - and diversify for each tag - the password and PACK from its delivery state at tag issuing.

10.8 READ

The READ command requires a start page address, and returns the 16 bytes of four NTAG I²C *plus* pages. For example, if address (Addr) is 03h then pages 03h, 04h, 05h, 06h are returned. Special conditions apply if the READ command address is near the end of the accessible memory area. For details on those cases and the command structure, refer to Figure 24 and Table 27.

Table 28 shows the required timing.

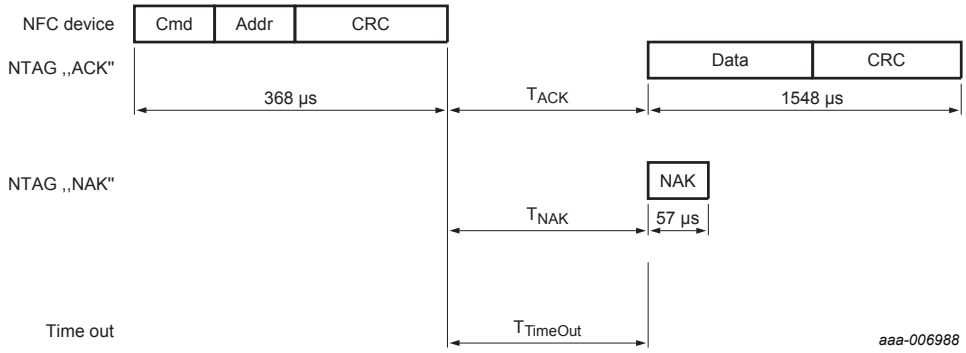


Figure 24. READ command

Table 27. READ command

Name	Code	Description	Length
Cmd	30h	read four pages	1 byte
Addr	-	start page address	1 byte
CRC	-	CRC according to Ref. 1	2 bytes
Data	-	Data content of the addressed pages	16 bytes
NAK	see Table 17	see Section 10.3	4 bit

Table 28. READ timing

These times exclude the end of communication of the NFC device.

	$T_{ACK/NAK}$ min	$T_{ACK/NAK}$ max	$T_{TimeOut}$
READ	n=9[1]	$T_{TimeOut}$	5 ms

[1] Refer to Section 10.2 "Timing".

In the initial state of NTAG I²C *plus*, all memory pages are allowed as Addr parameter to the READ command:

- Page address from 00h to E9h and pages ECh and EDh for NTAG I²C *plus* 1k and 2k
- Page address from 00h to FFh (Sector 1) for NTAG I²C *plus* 2k only
- SRAM buffer address when pass-through mode is enabled

Addressing a start memory page beyond the limits above results in a NAK response from NTAG I²C *plus*.

In case a READ command addressing start with a valid memory area but extends over an invalid memory area, the content of the invalid memory area will be reported as 00h.

10.9 FAST_READ

The FAST_READ command requires a start page address and an end page address and returns all n*4 bytes of the addressed pages. For example, if the start address is 03h and the end address is 07h, then pages 03h, 04h, 05h, 06h and 07h are returned.

For details on those cases and the command structure, refer to Figure 25 and Table 29.

Table 30 shows the required timing.

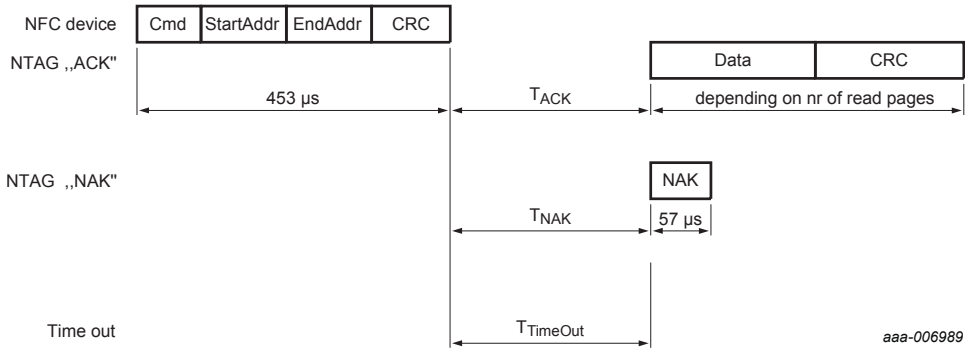


Figure 25. FAST_READ command

Table 29. FAST_READ command

Name	Code	Description	Length
Cmd	3Ah	read multiple pages	1 byte
StartAddr	-	start page address	1 byte
EndAddr	-	end page address	1 byte
CRC	-	CRC according to Ref. 1	2 bytes
Data	-	data content of the addressed pages	n*4 bytes
NAK	see Table 17	see Section 10.3	4 bit

Table 30. FAST_READ timing

These times exclude the end of communication of the NFC device.

	$T_{ACK/NAK}$ min	$T_{ACK/NAK}$ max	$T_{TimeOut}$
FAST_READ	n=9[1]	$T_{TimeOut}$	5 ms

[1] Refer to Section 10.2 "Timing".

In the initial state of NTAG I²C *plus*, all memory pages are allowed as StartAddr parameter to the FAST_READ command:

- Page address from 00h to E9h and pages ECh and EDh for NTAG I²C *plus* 1k and 2k
- Page address from 00h to FFh (Sector 1) for NTAG I²C *plus* 2k only
- SRAM buffer address when pass-through mode is enabled

If the start addressed memory page (StartAddr) is outside of accessible area, NTAG I²C *plus* replies a NAK.

In case the FAST_READ command starts with a valid memory area but extends over an invalid memory area, the content of the invalid memory area will be reported as 00h.

The EndAddr parameter must be equal to or higher than the StartAddr.

Remark: The FAST_READ command is able to read out the entire memory of one sector with one command. Nevertheless, the receive buffer of the NFC device must be able to handle the requested amount of data as no chaining is possible.

10.10 WRITE

The WRITE command requires a page address, and writes 4 bytes of data into the addressed NTAG I²C *plus* page. The WRITE command is shown in Figure 26 and Table 31.

Table 32 shows the required timing.

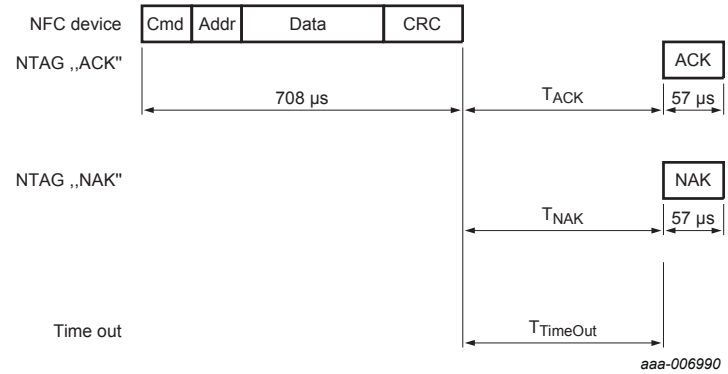


Figure 26. WRITE command

Table 31. WRITE command

Name	Code	Description	Length
Cmd	A2h	write one page	1 byte
Addr	-	page address	1 byte
Data	-	data	4 bytes
CRC	-	CRC according to Ref. 1	2 bytes
NAK	see Table 17	see Section 10.3	4 bit

Table 32. WRITE timing

These times exclude the end of communication of the NFC device.

	$T_{ACK/NAK}$ min	$T_{ACK/NAK}$ max	$T_{TimeOut}$
WRITE	n=9[1]	$T_{TimeOut}$	5 ms

[1] Refer to Section 10.2 "Timing".

In the initial state of NTAG I²C *plus*, the following memory pages are valid Addr parameters to the WRITE command:

- Page address from 02h to E9h (Sector 0) for NTAG I²C *plus* 1k and 2k
- Page address from 00h to FFh (Sector 1) for NTAG I²C *plus* 2k
- SRAM buffer addresses when pass-through mode is enabled

Addressing a memory page beyond the limits above results in a NAK response from NTAG I²C *plus*.

Pages that are locked against writing cannot be reprogrammed using any write command. The locking mechanisms include static and dynamic lock bits, as well as the locking of the configuration pages.

10.11 FAST_WRITE

The FAST_WRITE allows to write data in ACTIVE state to the complete SRAM (64 bytes) in pass-through mode, and requires the start block address (F0h), end address (FFh) and writes 64 bytes of data into the NTAG I²C *plus* SRAM. The FAST_WRITE command is shown in Figure 26 and Table 31.

WARNING: Data is written directly to SRAM. If received CRC at the end of transmission is wrong and response was a NAK, received (corrupted) data is still in SRAM. Hence it is recommended to implement a protocol on top to ensure data integrity (e.g. include own CRC at the end of the payload) when using SRAM.

Table 32 shows the required timing.

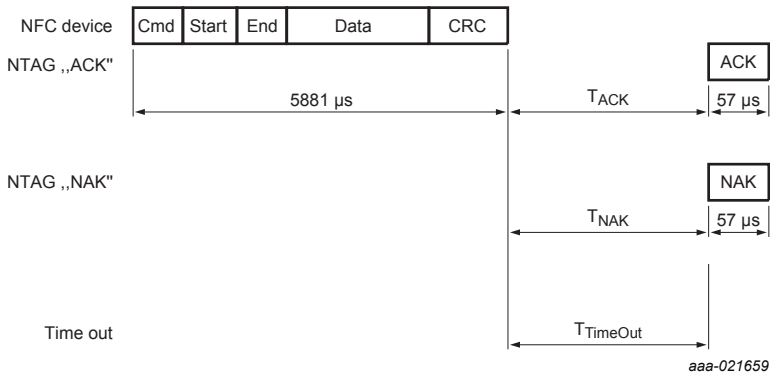


Figure 27. FAST_WRITE command

Table 33. FAST_WRITE command

Name	Code	Description	Length
Cmd	A6h	write complete SRAM	1 byte
START_ADDR	F0h	start SRAM in pass-through mode	1 byte
END_ADDR	FFh	end SRAM in pass-through mode	1 byte
Data	-	data	64 bytes
-	CRC	CRC according to Ref. 1	2 bytes
ACK	see Table 17	see Section 10.3	4 bit
NAK	see Table 17	see Section 10.3	4 bit

Table 34. FAST_WRITE timing

These times exclude the end of communication of the NFC device.

	$T_{ACK/NAK}$ min	$T_{ACK/NAK}$ max	$T_{TimeOut}$
FAST_WRITE	n=9[1]	$T_{TimeOut}$	5 ms

[1] Refer to Section 10.2 "Timing".

10.12 SECTOR SELECT

The SECTOR SELECT command consists of two commands packet: the first one is the SECTOR SELECT command (C2h), FFh and CRC. Upon an ACK answer from the Tag, the second command packet needs to be issued with the related sector address to be accessed and 3 bytes RFU.

To successfully access to the requested memory sector, the tag shall issue a passive ACK, which is sending NO REPLY for more than 1 ms after the CRC of the second command set.

The SECTOR SELECT command is shown in Figure 28 and Table 35.

Table 36 shows the required timing.

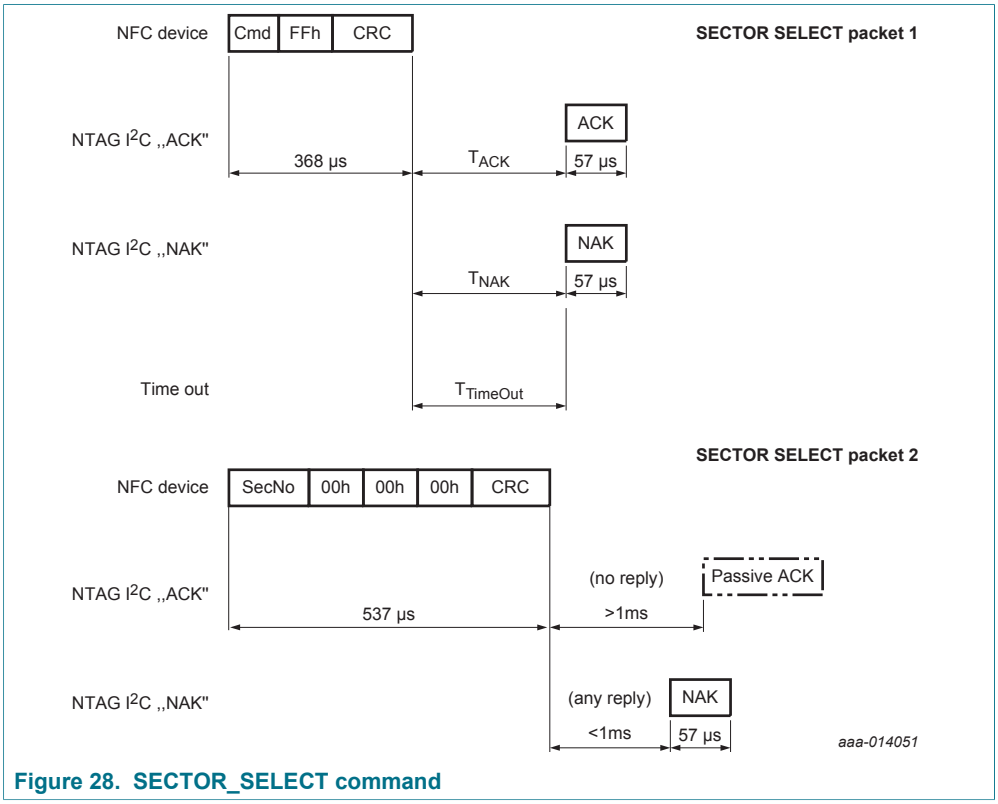


Figure 28. SECTOR_SELECT command

Table 35. SECTOR_SELECT command

Name	Code	Description	Length
Cmd	C2h	sector select	1 byte

Name	Code	Description	Length
FFh	-		1 byte
CRC	-	CRC according to Ref. 1	2 bytes
SecNo	-	Memory sector to be selected (00h - FEh)	1 byte
NAK	see Table 17	see Section 10.3	4 bit

Table 36. SECTOR_SELECT timing

These times exclude the end of communication of the NFC device.

	$T_{ACK/NAK}$ min	$T_{ACK/NAK}$ max	$T_{TimeOut}$
SECTOR_SELECT	n=9[1]	$T_{TimeOut}$	5 ms

[1] Refer to Section 10.2 "Timing".

11 Communication and arbitration between NFC and I²C interface

If both interfaces are powered by their corresponding source, only one interface shall have access to the memory according to the "first-come, first-serve" principle.

In NS_REG, the two status bits I2C_LOCKED and RF_LOCKED reflect the status of the NTAG I²C *plus* memory access and indicate which interface is locking the memory access. At power-on, both bits are 0b, setting the arbitration in idle mode.

In the case arbiter locks to the I²C interface, an NFC device can still read the session registers. If the NFC state machine is in ACTIVE state, only the SECTOR SELECT command is allowed. But any other command requiring EEPROM access like READ or WRITE is handled as an illegal command and replied to with a NAK value.

In the case where the memory access is locked to the NFC interface, the I²C host can still access the session register, by issuing a 'Register READ/WRITE' command. All other read or write commands will be replied to with a NACK to the I²C host.

11.1 Pass-through mode not activated

PTHRU_ON_OFF = 0b (see Table 14) indicates non-pass-through mode.

11.1.1 I²C interface access

If the tag is in the IDLE or HALT state (NFC state after POR or HALT-command) and the correct I²C slave address of NTAG I²C *plus* is received following the START condition, the bit I2C_LOCKED will be automatically set to 1b. If I2C_LOCKED = 1b, the I²C interface has access to the tag memory and the tag will respond with a NACK to any memory READ/WRITE command on the NFC interface other than reading the session register bytes during this time.

I2C_LOCKED must be either reset to 0b at the end of the I²C sequence or will be cleared automatically after the end of the watch dog timer.

11.1.2 NFC interface access

The arbitration will allow the NFC interface read and write accesses to EEPROM only when I2C_LOCKED is set to 0b.

RF_LOCKED is automatically set to 1b if the tag receives a valid command (EEPROM Access Commands) on the NFC interface. If RF_LOCKED = 1b, the tag is locked to the NFC interface and will not respond to any command from the I²C interface other than READ register command (see Table 14).

RF_LOCKED is automatically set to 0b in one of the following conditions

- At POR or if the NFC field is switched off
- If the tag is set to the HALT state with a HALT command on the NFC interface
- If the memory access command is finished on the NFC interface

When the NFC interface has read the last page of the NDEF message specified in LAST_NDEF_BLOCK (see Table 13 and Table 14) the bit NDEF_DATA_READ - in the register NS_REG see Table 14 - is set to 1b and indicates to the I²C interface that, for example, new NDEF data can be written.

11.2 SRAM buffer mapping with Memory Mirror enabled

With SRAM_MIRROR_ON_OFF= 1b, the SRAM buffer mirroring is enabled. This mode cannot be combined with the pass-through mode (see Section 11.3).

With the memory mirror enabled, the SRAM is now mapped into the user memory from the NFC interface perspective using the SRAM mirror lower page address specified in SRAM_MIRROR_BLOCK byte (Table 13 and Table 14). See Table 37 (NTAG I²C *plus* 1k) and Table 38 (NTAG I²C *plus* 2k) for an illustration of this SRAM memory mapping when SRAM_MIRROR_BLOCK is set to 01h.

Password protection to this mapped SRAM may be enabled by enabling password authentication and setting SRAM_PROT bit to 1b.

In contrary to password protection, for read only locking there are no special lock bits for the SRAM. Whenever user EEPROM blocks are locked to read-only with static and/or dynamic lock bits, potential mirrored SRAM blockes are read-only, too.

The tag must be VCC powered to make this mode work, because without VCC, the SRAM will not be accessible via NFC powered only.

When mapping the SRAM buffer to the user memory, the user shall be aware that all data written into the SRAM will be lost once the NTAG I²C *plus* is no longer powered from the I²C side (as SRAM is a volatile memory).

Table 37. Illustration of the SRAM memory addressing via the NFC interface (with SRAM_MIRROR_ON_OFF set to 1b and SRAM_MIRROR_BLOCK set to 01h) for the NTAG I²C *plus* 1k

Sector address	Page address		Byte number within a page				Access cond. ACTIVE state	Access cond. AUTH. state
	Dec.	Hex.	0	1	2	3		
0	0	00h	Serial number (UID)				READ	
	1	01h	Serial number (UID)			Internal	READ	
	2	02h	Internal		Static lock bytes		READ/R&W	
	3	03h	Capability Container (CC)				READ&WRITE	
	4	04h	SRAM				READ&WRITE	
	...	...						
	19	13h						
	...	...	Unprotected user memory				READ&WRITE	
	AUTH0	AUTH0	Protected user memory				READ	READ&WRITE
	...	...						
	225	E1h						
	226	E2h	Dynamic lock bytes			00h	R&W/READ	
	227	E3h	RFU	RFU	RFU	AUTH0	READ	READ&WRITE
	228	E4h	ACCESS	RFU	RFU	RFU	READ	READ&WRITE
	229	E5h	PWD				READ	READ&WRITE
	230	E6h	PACK		RFU	RFU	READ	READ&WRITE
	231	E7h	PT_I2C	RFU	RFU	RFU	READ	READ&WRITE
	232	E8h	Configuration registers				see 8.3.12	
	233	E9h						

Sector address	Page address		Byte number within a page				Access cond. ACTIVE state	Access cond. AUTH. state
	Dec.	Hex.	0	1	2	3		
	234	EAh	Invalid access - returns NAK				n.a.	
	235	EBh						
	236	ECh	Session registers				see 8.3.12	
	237	EDh						
	238	EEh	Invalid access - returns NAK				n.a.	
	239	EFh						
	240	F0h	Invalid access - returns NAK				n.a.	
	...	...						
	255	FFh						
1	...	...	Invalid access - returns NAK				n.a.	
2	...	...	Invalid access - returns NAK				n.a.	
3	0	00h	Invalid access - returns NAK				n.a.	
	...	...						
	248	F8h	Session registers				see 8.3.12	
	249	F9h						
	...	...	Invalid access - returns NAK				n.a.	
	255	FFh						

Table 38. Illustration of the SRAM memory addressing via the NFC interface (with SRAM_MIRROR_ON_OFF set to 1b and SRAM_MIRROR_BLOCK set to 01h) for the NTAG I²C *plus* 2k

Sector address	Page address		Byte number within a page				Access cond. ACTIVE state	Access cond. AUTH. state
	Dec.	Hex.	0	1	2	3		
0	0	00h	Serial number (UID)				READ	
	1	01h	Serial number (UID)			Internal	READ	
	2	02h	Internal		Static lock bytes		READ/R&W	
	3	03h	Capability Container (CC)				READ&WRITE	
	4	04h	SRAM				READ&WRITE	
	...	...						
	19	13h						
	...	...	Unprotected user memory				READ&WRITE	
	AUTH0	AUTH0	Protected user memory				READ	READ&WRITE
	...	...						
	225	E1h						
	226	E2h	Dynamic lock bytes			00h	R&W/READ	
	227	E3h	RFU	RFU	RFU	AUTH0	READ	READ&WRITE

Sector address	Page address		Byte number within a page				Access cond. ACTIVE state	Access cond. AUTH. state
	Dec.	Hex.	0	1	2	3		
	228	E4h	ACCESS	RFU	RFU	RFU	READ	READ&WRITE
	229	E5h	PWD				READ	READ&WRITE
	230	E6h	PACK		RFU	RFU	READ	READ&WRITE
	231	E7h	PT_I2C	RFU	RFU	RFU	READ	READ&WRITE
	232	E8h	Configuration registers				see 8.3.12	
	233	E9h						
	234	EAh	Invalid access - returns NAK				n.a.	
	235	EBh						
	236	ECh	Session registers				see 8.3.12	
	237	EDh						
	238	EEh	Invalid access - returns NAK				n.a.	
	239	EFh						
	240	F0h	Invalid access - returns NAK				n.a.	
	...	...						
	255	FFh						
1	0	00h	(Un-)protected user memory				READ&WRITE	
	...	...						
	255	FFh						
2	...	...	Invalid access - returns NAK				n.a.	
3	0	00h	Invalid access - returns NAK				n.a.	
	...	...						
	248	F8h	Session registers				see 8.3.12	
	249	F9h						
	...	...	Invalid access - returns NAK				n.a.	
	255	FFh						

11.3 Pass-through mode

PTHRU_ON_OFF = 1b (see Table 14) enables and indicates pass-through mode.

Password protection for pass-through mode may be enabled by enabling password authentication and setting SRAM_PROT bit to 1b.

To handle large amount of data transfer from one interface to the other, NTAG I²C *plus* offers the pass-through mode where data is transferred via a 64 byte SRAM. This buffer offers fast write access and unlimited write endurance as well as an easy handshake mechanism between the two interfaces.

This buffer is mapped directly at the end of the Sector 0 of NTAG I²C *plus*.

In both directions, the principle of access to the SRAM buffer via the NFC and I²C interface is exactly the same (see Section 11.3.2 and Section 11.3.3).

The data flow direction must be set with the TRANSFER_DIR bit (see Table 14) within the current communication session using the session registers (it can only be set via the I²C interfaces) or for the configuration bits after POR (in this case both NFC and I²C interface can set it). This pass-through direction setting avoids locking the memory access during the data transfer from one interface to the SRAM buffer.

The pass-through mode can only be enabled via I²C interface when both interfaces are powered. The PTHRU_ON_OFF bit, located in the session registers NC_REG (see Section 8.3.12), needs to be set to 1b. In case one interface powers off, the pass-through mode is disabled automatically.

NTAG I²C *plus* introduces in addition to the FAST_READ command a FAST_WRITE command. With this new command in ACTIVE state whole SRAM can be written at once, which improves the total pass-through performance significantly.

For more information read related application note Ref. 8.

11.3.1 SRAM buffer mapping

In pass-through mode, the SRAM of NTAG I²C *plus* is mirrored to pages F0h to FFh of Sector 0.

The last page/block of the SRAM (page FFh) is used as the terminator page. Once the terminator page/block in the respective interfaces is read/written, the control would be transferred to other interface (NFC/I²C) - see Section 11.3.2 and Section 11.3.3 for more details.

Accordingly, the application can align on the reader and host side to transfer 16/32/48/64 bytes of data in one pass-through step by only using the last blocks/page of the SRAM buffer.

For best performance in addition to the FAST_READ, the FAST_WRITE command should be used.

Table 39. Illustration of the SRAM memory addressing via the NFC interface in pass-through mode (PTHRU_ON_OFF set to 1b) for the NTAG I²C 1k

Sector address	Page address		Byte number within a page				Access cond. ACTIVE state	Access cond. AUTH. state
	Dec.	Hex.	0	1	2	3		
0	0	00h	Serial number (UID)				READ	
	1	01h	Serial number (UID)			Internal	READ	
	2	02h	Internal		Static lock bytes		READ/R&W	
	3	03h	Capability Container (CC)				READ&WRITE	
	4	04h	Unprotected user memory				READ&WRITE	
	...	...						
	AUTH0	AUTH0	Protected user memory				READ	READ&WRITE
	...	...						
	225	E1h						
	226	E2h	Dynamic lock bytes			00h	R&W/READ	
	227	E3h	RFU	RFU	RFU	AUTH0	READ	READ&WRITE
	228	E4h	ACCESS	RFU	RFU	RFU	READ	READ&WRITE
	229	E5h	PWD				READ	READ&WRITE

Sector address	Page address		Byte number within a page				Access cond. ACTIVE state	Access cond. AUTH. state
	Dec.	Hex.	0	1	2	3		
	230	E6h	PACK		RFU	RFU	READ	READ&WRITE
	231	E7h	PT_I2C	RFU	RFU	RFU	READ	READ&WRITE
	232	E8h	Configuration registers				see 8.3.12	
	233	E9h						
	234	EAh	Invalid access - returns NAK				n.a.	
	235	EBh						
	236	ECh	Session registers				see 8.3.12	
	237	EDh						
	238	EEh	Invalid access - returns NAK				n.a.	
	239	EFh						
	240	F0h	SRAM				READ&WRITE	
	...	...						
	255	FFh						
1	...	...	Invalid access - returns NAK				n.a.	
2	...	...	Invalid access - returns NAK				n.a.	
3	0	00h	Invalid access - returns NAK				n.a.	
	...	...						
	248	F8h	Session registers				see 8.3.12	
	249	F9h						
	...	...	Invalid access - returns NAK				n.a.	
	255	FFh						

Table 40. Illustration of the SRAM memory addressing via the NFC interface in pass-through mode (PTHRU_ON_OFF set to 1b) for the NTAG I²C 2k

Sector address	Page address		Byte number within a page				Access cond. ACTIVE state	Access cond. AUTH. state
	Dec.	Hex.	0	1	2	3		
0	0	00h	Serial number (UID)				READ	
	1	01h	Serial number (UID)			Internal	READ	
	2	02h	Internal		Static lock bytes		READ/R&W	
	3	03h	Capability Container (CC)				READ&WRITE	
	4	04h	Unprotected user memory				READ&WRITE	
	...	...						
	AUTH0	AUTH0	Protected user memory				READ	READ&WRITE
	...	...						
	225	E1h						

Sector address	Page address		Byte number within a page				Access cond. ACTIVE state	Access cond. AUTH. state
	Dec.	Hex.	0	1	2	3		
	226	E2h	Dynamic lock bytes			00h	R&W/READ	
	227	E3h	RFU	RFU	RFU	AUTH0	READ	READ&WRITE
	228	E4h	ACCESS	RFU	RFU	RFU	READ	READ&WRITE
	229	E5h	PWD				READ	READ&WRITE
	230	E6h	PACK		RFU	RFU	READ	READ&WRITE
	231	E7h	PT_I2C	RFU	RFU	RFU	READ	READ&WRITE
	232	E8h	Configuration registers				see 8.3.12	
	233	E9h						
	234	EAh	Invalid access - returns NAK				n.a.	
	235	EBh						
	236	ECh	Session registers				see 8.3.12	
	237	EDh						
	238	EEh	Invalid access - returns NAK				n.a.	
	239	EFh						
	240	F0h	SRAM				READ&WRITE	
	...	...						
	255	FFh						
1	0	00h	(Un-)protected user memory				READ&WRITE	
	...	...						
	255	FFh						
2	...	...	Invalid access - returns NAK				n.a.	
3	0	00h	Invalid access - returns NAK				n.a.	
	...	...						
	248	F8h	Session registers				see 8.3.12	
	249	F9h						
	...	...	Invalid access - returns NAK				n.a.	
	255	FFh						

11.3.2 NFC to I²C data transfer

If the NFC interface is enabled (RF_LOCKED = 1b) and data is written to the terminator page FFh of the SRAM via the NFC interface, at the end of the WRITE command, bit SRAM_I2C_READY is set to 1b and bit RF_LOCKED is set to 0b automatically, and the NTAG I²C *plus* is locked to the I²C interface.

To signal the host that data is ready to be read following mechanisms are in place:

- The host polls/reads bit SRAM_I2C_READY from NS_REG (see Table 14) to know if data is ready in SRAM

- A trigger on the FD pin indicates to the host that data is ready to be read from SRAM. This feature can be enabled by programming bits 5:2 (FD_OFF, FD_ON) of the NC_REG appropriately (see Table 13)

This is illustrated in the Figure 29.

If the tag is addressed with the correct I²C slave address, the I2C_LOCKED bit is automatically set to 1b (according to the interface arbitration). After a READ from the terminator page of the SRAM, bit SRAM_I2C_READY and bit I2C_LOCKED are automatically reset to 0b, and the tag returns to the arbitration idle mode where, for example, further data from the NFC interface can be transferred.

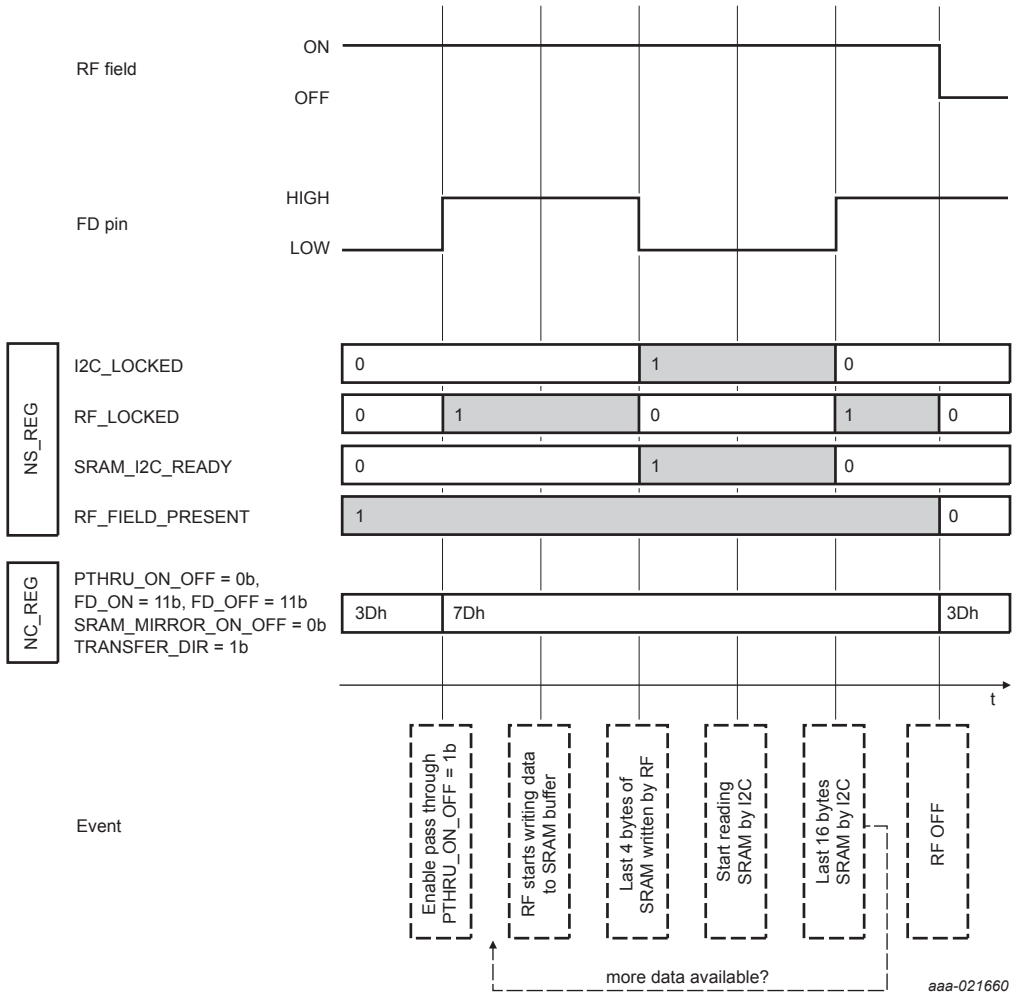


Figure 29. Illustration of the Field detection feature in combination with the pass-through mode for data transfer from NFC to I²C

11.3.3 I²C to NFC data transfer

If the I²C interface is enabled (I2C_LOCKED is 1b) and data is written to the terminator block FBh of the SRAM via the I²C interface, at the end of the WRITE command, bit SRAM_RF_READY is set to 1b and bit I2C_LOCKED is automatically reset to 0b to set the tag in the arbitration idle state.

The RF_LOCKED bit is then automatically set to 1b (according to the interface arbitration). After a READ or FAST_READ command involving the terminator page of the SRAM, bit SRAM_RF_READY and bit RF_LOCKED are automatically reset to 0b allowing the I²C interface to further write data into the SRAM buffer.

To signal to the host that further data is ready to be written, the following mechanisms are in place:

- The NFC interface polls/reads the bit SRAM_RF_READY from NS_REG (see Table 14) to know if new data has been written by the I²C interface in the SRAM
- A trigger on the FD pin indicates to the host that data has been read from SRAM by the NFC interface. This feature can be enabled by programming bits 5:2 (FD_OFF, FD_ON) of the NC_REG appropriately (see Table 13)

The above mechanism is illustrated in the Figure 30.

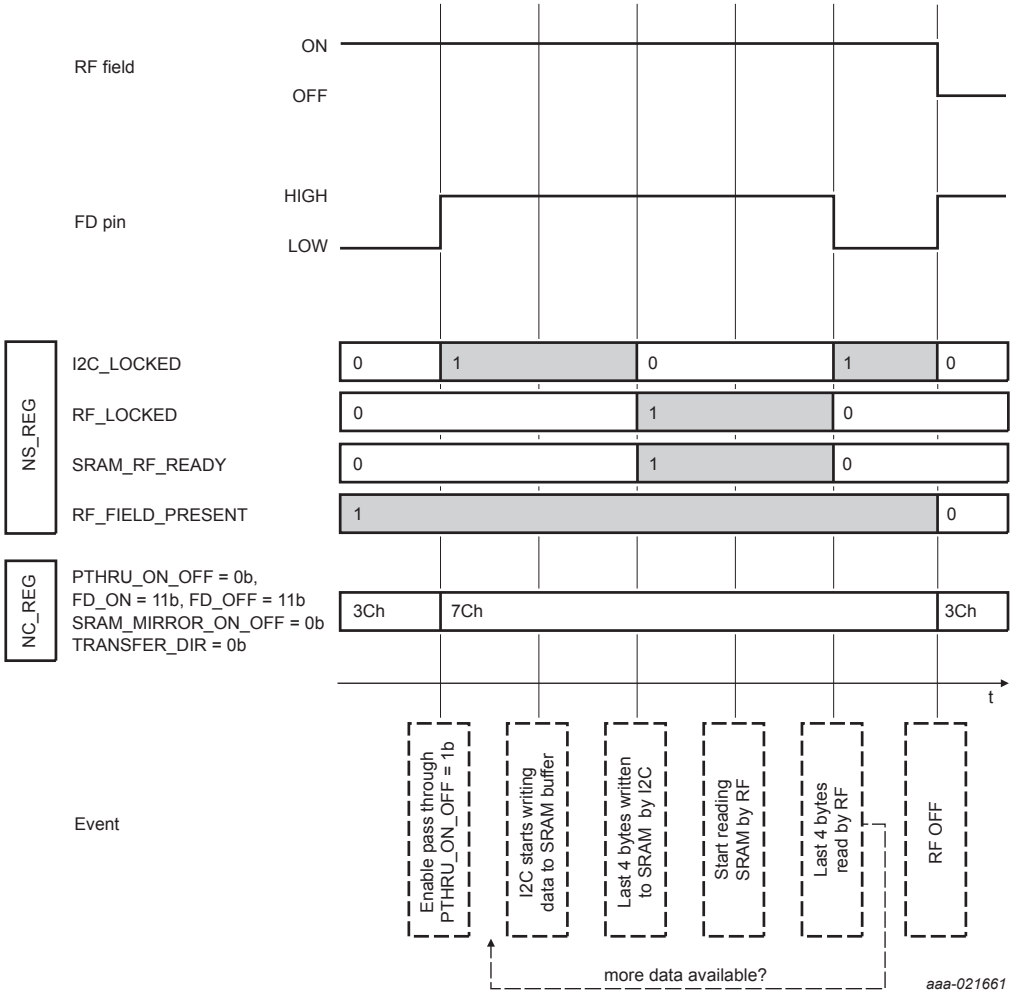


Figure 30. Illustration of the Field detection signal feature in combination with pass-through mode for data transfer from I²C to NFC

12 Limiting values

Exceeding the limits of one or more values in reference may cause permanent damage to the device. Exposure to limiting values for extended periods may affect device reliability.

Table 41. Limiting values

In accordance with the Absolute Maximum Rating System (IEC 60134).[1][2]

Symbol	Parameter	Conditions	Min	Max	Unit
T_{stg}	storage temperature		-55	+125	°C
$T_{j(max)}$	maximum junction temperature		-	+105	°C
V_{ESD}	electrostatic discharge voltage (Human Body model)	[3]	-	2	kV
V_{ESD}	electrostatic discharge voltage (Charge Device model)	[4]	-	1	kV
V_{DD}	supply voltage	on pin VCC	-0.5	4.6	V
V_i	input voltage	on pin FD, SDA, SCL	-0.5	4.6	V
I_i	input current	on pin LA, LB	-	40	mA
$V_{i(RF)}$	RF input voltage	on pin LA, LB	-	4.6	V_{peak}

[1] Stresses above one or more of the limiting values may cause permanent damage to the device.
[2] Exposure to limiting values for extended periods may affect device reliability.
[3] ANSI/ESDA/JEDEC JS-001
[4] ANSI/ESDA/JEDEC JS-002

13 Characteristics

13.1 Electrical characteristics

Table 42. Characteristics

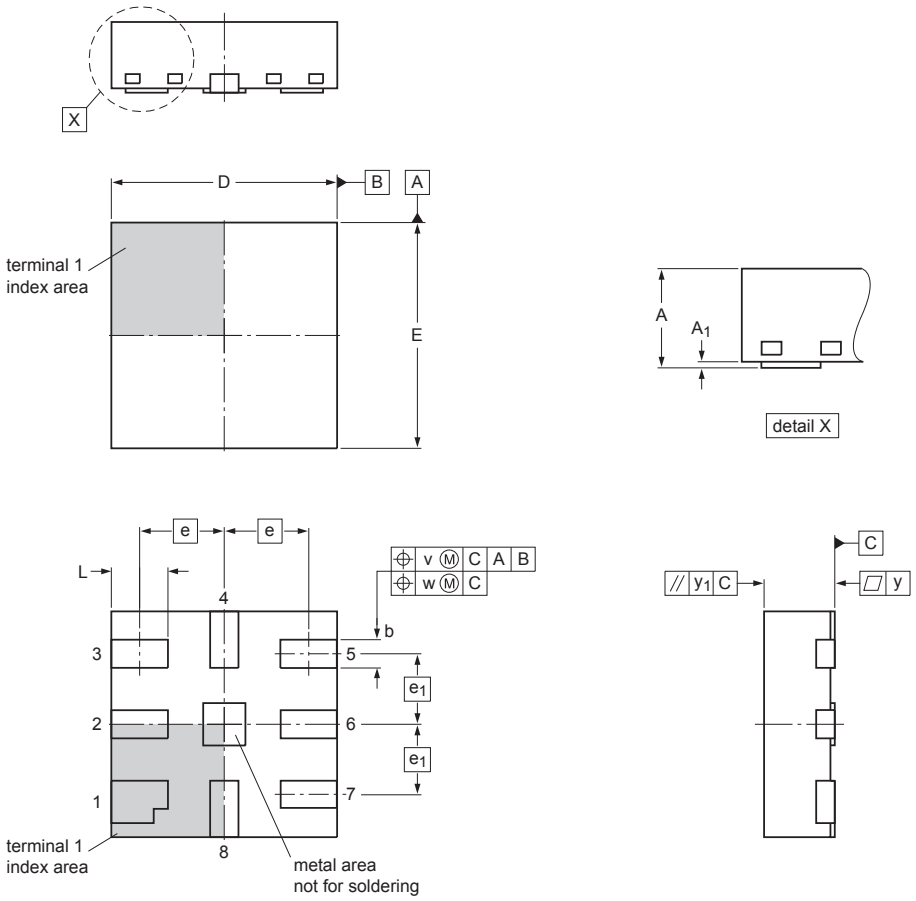
Symbol	Parameter	Conditions	Min	Typ	Max	Unit
C_i	input capacitance	LA - LB, on chip - C_{IC}, f=13.56 MHz, V_{LA-LB}=2.4 V_{RMS}	44	50	56	pF
f_i	input frequency		-	13.56	-	MHz
T_{amb}	operating ambient temperature		-40	25	+105 [1]	°C
R_{TH_JA}	thermal resistance	JEDEC 2s2p board and XQFN8 package	-	150	-	K/W
R_{TH_JA}	thermal resistance	JEDEC 2s2p board and TSSOP8 package	-	211	-	K/W
R_{TH_JA}	thermal resistance	JEDEC 2s2p board and SO8 package	-	115	-	K/W
Energy harvesting characteristics						
$V_{out,max}$	output voltage	generated at the V_{out} pin, Class 5 antenna, 14 A/m, load current 1 mA	[2]	-	3.3	V
I²C interface characteristics						
V_{CC}	supply voltage	supplied via V_{CC} only	1.67	-	3.6	V
I_{DD}	supply current	V_{CC}=1.8 V I²C; idle bus	-	160	-	µA
		V_{CC}=3.3 V I²C; idle bus	-	195	-	µA
I_{DD}	supply current	V_{CC}=1.8 V I²C@400KHz	-	-	185	µA
		V_{CC}=2.5 V I²C@400KHz	-	-	210	µA
		V_{CC}=3.3 V I²C@400KHz	-	-	240	µA
I²C pin characteristics						
V_{OL}	LOW-level output voltage	I_{OL}= 3 mA; V_{CC} > 2 V	-	-	0.4	V
		I_{OL}= 2 mA; V_{CC} < 2 V	-	-	0.2*V_{CC}	V
V_{IH}	HIGH-level input voltage		0.7*V_{CC}	-	-	V
V_{IL}	LOW-level input voltage		-	-	0.3*V_{CC}	V
C_i	input capacitance	SCL and SDA pin	-	2.4	-	pF
I_L	leakage current	0 V and $V_{CC,max}$	-	-	10	µA
t_{high}	SCL high time	fast mode 400 kHz	950	-	-	ns
FD pin characteristics						
V_{OL}	LOW-level output voltage	I_{OL}= 4 mA; V_{CC} > 2 V	-	-	0.4	V
		I_{OL}= 3 mA; V_{CC} < 2 V	-	-	0.2*V_{CC}	V
I_L	leakage current		-	1.5	10	µA
EEPROM characteristics						

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
t_{ret}	retention time	T_{amb}	20	50	-	year
$N_{endu(W)}$	write endurance	T_{amb}	200000	-	-	cycle
$N_{endu(W)}$	write endurance	-40°C to 95°C	500000	1000000	-	cycle

[1] Dependent on PCB design and operating conditions
[2] Minimum value depends on available field strength and load current conditions. For details refer to [7] AN11578 NTAG I²C Energy Harvesting

14 Package outline

XQFN8: plastic, extremely thin quad flat package; no leads; 8 terminals; body 1.6 x 1.6 x 0.5 mm **SOT902-3**



Dimensions

Unit		A	A_1	b	D	E	e	e_1	L	v	w	y	y_1
mm	max	0.5	0.05	0.25	1.65	1.65			0.45				
	nom			0.20	1.60	1.60	0.6	0.5	0.40	0.1	0.05	0.05	0.05
	min		0.00	0.15	1.55	1.55			0.35				

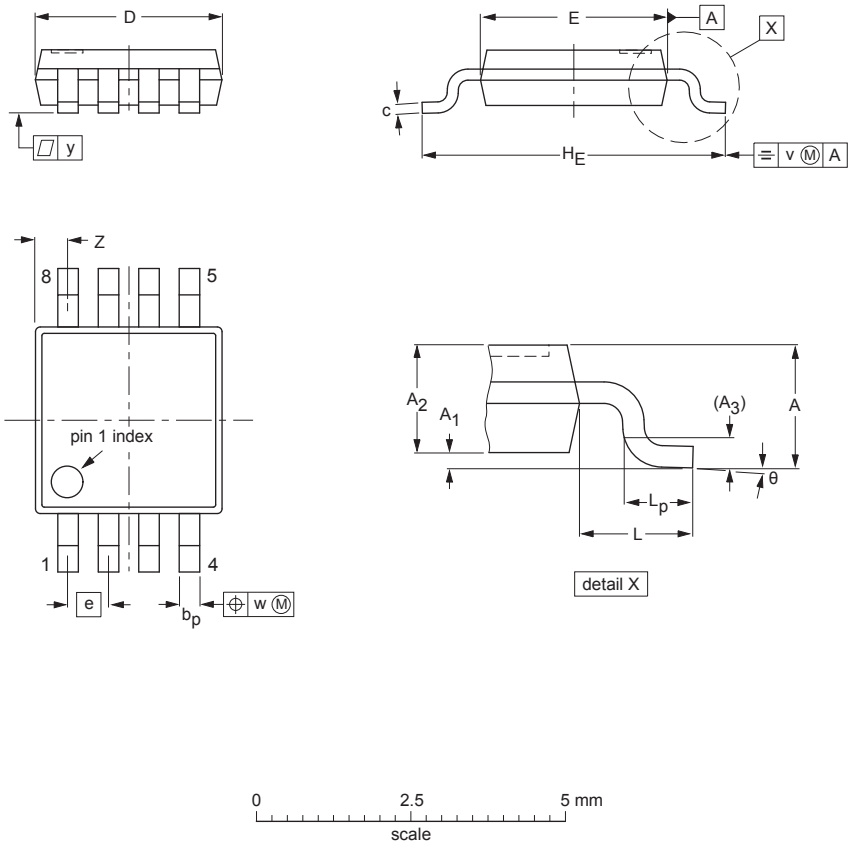
Note
1. Plastic or metal protrusions of 0.075 mm maximum per side are not included.

sot902-3_po

Outline version	References				European projection	Issue date
	IEC	JEDEC	JEITA			
SOT902-3	- - -	MO-255	- - -			~~11-08-16~~ 11-08-18

Figure 31. Package outline SOT902-3 (XQFN8)

TSSOP8: plastic thin shrink small outline package; 8 leads; body width 3 mm **SOT505-1**



DIMENSIONS (mm are the original dimensions)

UNIT	A max.	A_1	A_2	A_3	b_p	c	$D^{(1)}$	$E^{(2)}$	e	H_E	L	L_p	v	w	y	$Z^{(1)}$	θ
mm	1.1	0.15 0.05	0.95 0.80	0.25	0.45 0.25	0.28 0.15	3.1 2.9	3.1 2.9	0.65	5.1 4.7	0.94	0.7 0.4	0.1	0.1	0.1	0.70 0.35	6° 0°

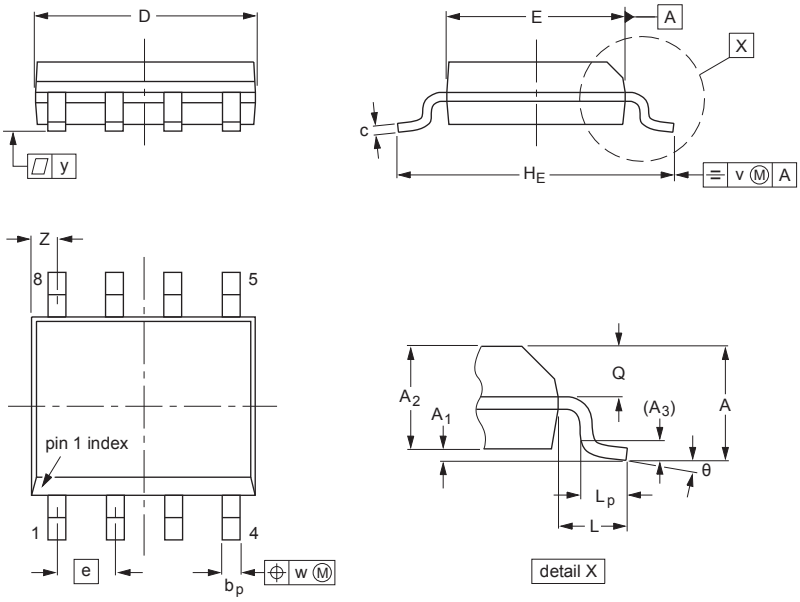
Notes

1. Plastic or metal protrusions of 0.15 mm maximum per side are not included.
2. Plastic or metal protrusions of 0.25 mm maximum per side are not included.

OUTLINE VERSION	REFERENCES				EUROPEAN PROJECTION	ISSUE DATE
	IEC	JEDEC	JEITA			
SOT505-1						~~99-04-09~~ 03-02-18

Figure 32. Package outline SOT505-1 (TSSOP8)

SO8: plastic small outline package; 8 leads; body width 3.9 mm **SOT96-1**



DIMENSIONS (inch dimensions are derived from the original mm dimensions)

UNIT	A max.	A_1	A_2	A_3	b_p	c	$D^{(1)}$	$E^{(2)}$	e	H_E	L	L_p	Q	v	w	y	$Z^{(1)}$	θ
mm	1.75	0.25 0.10	1.45 1.25	0.25	0.49 0.36	0.25 0.19	5.0 4.8	4.0 3.8	1.27	6.2 5.8	1.05	1.0 0.4	0.7 0.6	0.25	0.25	0.1	0.7 0.3	8° 0°
inches	0.069	0.010 0.004	0.057 0.049	0.01	0.019 0.014	0.0100 0.0075	0.20 0.19	0.16 0.15	0.05	0.244 0.228	0.041	0.039 0.016	0.028 0.024	0.01	0.01	0.004	0.028 0.012	

Notes

1. Plastic or metal protrusions of 0.15 mm (0.006 inch) maximum per side are not included.
2. Plastic or metal protrusions of 0.25 mm (0.01 inch) maximum per side are not included.

OUTLINE VERSION	REFERENCES				EUROPEAN PROJECTION	ISSUE DATE
	IEC	JEDEC	JEITA			
SOT96-1	076E03	MS-012				~~99-12-27~~ 03-02-18

Figure 33. Package outline SOT96-1 (SO8)

15 Handling information

CAUTION

This device is sensitive to ElectroStatic Discharge (ESD). Observe precautions for handling electrostatic sensitive devices.

Such precautions are described in the *ANSI/ESD S20.20, IEC/ST 61340-5, JESD625-A* or equivalent standards.

16 Abbreviations

Table 43. Abbreviations

Acronym	Description
ASID	Assembly Sequence ID
DBSN	Diffusion Batch Sequence number
POR	Power-On Reset

17 References

1. NFC Forum - Type 2 Tag Specification 1.0
   Technical Specification
2. ISO/IEC 14443 - Identification cards - Contactless integrated circuit cards - Proximity cards
   International Standard
3. I²C-bus specification and user manual
   NXP standard UM10204
   http://www.nxp.com/documents/user_manual/UM10204.pdf
4. NFC Forum - Activity 2.0
   Technical Specification
5. AN11276 NTAG Antenna Design Guide
   NXP Application Note
   http://www.nxp.com/documents/application_note/AN11276.pdf
6. AN11350 NTAG21x Originality Signature Validation
   NXP Application Note
   http://www.nxp.com/restricted_documents/53420/AN11350.pdf
7. AN11578 NTAG I²C Energy Harvesting
   NXP Application Note
   http://www.nxp.com/documents/application_note/AN11578.pdf
8. AN11579 How to use the NTAG I²C (*plus*) for bidirectional communication
   NXP Application Note
   http://www.nxp.com/documents/application_note/AN11579.pdf
9. AN11786 NTAG I²C *plus* Memory Configuration Options
   NXP Application Note
   http://www.nxp.com/documents/application_note/AN11786.pdf
10. XQFN8 - SOT902-3
    Package information
    https://www.nxp.com/docs/en/package-information/SOT902-3.pdf
11. TSSOP8 - SOT505-1
    Package information
    https://www.nxp.com/docs/en/package-information/SOT505-1.pdf
12. SO8 - SOT505-1
    Package information
    https://www.nxp.com/docs/en/package-information/SOT96-1.pdf
13. Certicom Research
    SEC 2: Recommended Elliptic Curve Domain Parameters V2.0

18 Revision history

Table 44. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
NT3H2111_2211 v. 3.5	20190507	Product data sheet	-	NT3H2111_2211 v. 3.4
Modifications:	• Information about I²C fail safe operation added • Link to detailed package specification on nxp.com added • Information added that tag does not need to be supplied via VCC for ED functionality added • Information added that reading NS_REG causes FD pin to be pulled low when configured for NFC field presence detection • Information that VOUT maybe used as field detect pin, when energy harvesting is not used • Typical idle current and FD pin leakage current added in characteristics (see Section 13) • RFU bits and bytes handling requirements added • Static and dynamic lock bits concequence to mirrored SRAM added • Editorial updates			
NT3H2111_2211 v. 3.4	20190108	Product data sheet	-	NT3H2111_2211 v. 3.3
Modifications:	• Package dimensions for XQFN8 in ordering information correcet according to package outline • CDM ESD limit added in limiting values table (see Section 12) • Editorial updates			
NT3H2111_2211 v. 3.3	20180808	Product data sheet	-	NT3H2111_2211 v. 3.2
Modifications:	• Info added, that ED pin is based on open-drain implementation • Warnings and recommendations related to I²C address added • Warning, that I²C read operations must be atomic added • T_j and thermal resistance added • Editorial updates			
NT3H2111_2211 v. 3.2	20171130	Product data sheet	-	NT3H2111_2211 v. 3.1
Modifications:	• Error in editorial update of V3.1 in Table 13, TRANSFER_DIR corrected			
NT3H2111_2211 v. 3.1	20171009	Product data sheet	-	v. 3.0
Modifications:	• Added info, that NTAG I²C *plus* now is NFC Forum certified • Endurance updated in Table 42 • Editorial updates			
NT3H2111_2211 v. 3.0	20160203	Product data sheet	-	-

19 Legal information

19.1 Data sheet status

Document status[1][2]	Product status[3]	Definition
Objective [short] data sheet	Development	This document contains data from the objective specification for product development.
Preliminary [short] data sheet	Qualification	This document contains data from the preliminary specification.
Product [short] data sheet	Production	This document contains the product specification.

[1] Please consult the most recently issued document before initiating or completing a design.
[2] The term 'short data sheet' is explained in section "Definitions".
[3] The product status of device(s) described in this document may have changed since this document was published and may differ in case of multiple devices. The latest product status information is available on the Internet at URL http://www.nxp.com.

19.2 Definitions

Draft — The document is a draft version only. The content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included herein and shall have no liability for the consequences of use of such information.

Short data sheet — A short data sheet is an extract from a full data sheet with the same product type number(s) and title. A short data sheet is intended for quick reference only and should not be relied upon to contain detailed and full information. For detailed and full information see the relevant full data sheet, which is available on request via the local NXP Semiconductors sales office. In case of any inconsistency or conflict with the short data sheet, the full data sheet shall prevail.

Product specification — The information and data provided in a Product data sheet shall define the specification of the product as agreed between NXP Semiconductors and its customer, unless NXP Semiconductors and customer have explicitly agreed otherwise in writing. In no event however, shall an agreement be valid in which the NXP Semiconductors product is deemed to offer functions and qualities beyond those described in the Product data sheet.

19.3 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors. In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory. Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification. Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products. NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Limiting values — Stress above one or more limiting values (as defined in the Absolute Maximum Ratings System of IEC 60134) will cause permanent damage to the device. Limiting values are stress ratings only and (proper) operation of the device at these or any other conditions above those given in the Recommended operating conditions section (if present) or the Characteristics sections of this document is not warranted. Constant or repeated exposure to limiting values will permanently and irreversibly affect the quality and reliability of the device.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at http://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

No offer to sell or license — Nothing in this document may be interpreted or construed as an offer to sell products that is open for acceptance or the grant, conveyance or implication of any license under any copyrights, patents or other industrial or intellectual property rights.

Quick reference data — The Quick reference data is an extract of the product data given in the Limiting values and Characteristics sections of this document, and as such is not complete, exhaustive or legally binding.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Non-automotive qualified products — Unless this data sheet expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications. In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

Translations — A non-English (translated) version of a document is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

19.4 Licenses

Purchase of NXP ICs with NFC technology

Purchase of an NXP Semiconductors IC that complies with one of the Near Field Communication (NFC) standards ISO/IEC 18092 and ISO/IEC 21481 does not convey an implied license under any patent right infringed by implementation of any of those standards. Purchase of NXP Semiconductors IC does not include a license to any NXP patent (or other IP right) covering combinations of those products with other products, whether hardware or software.

19.5 Trademarks

Notice: All referenced brands, product names, service names and trademarks are the property of their respective owners.

I²C-bus — logo is a trademark of NXP B.V.

NTAG — is a trademark of NXP B.V.

Tables

Figures

Contents

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

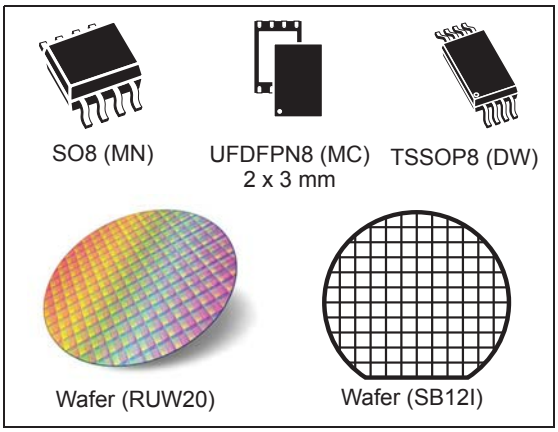
Date of release: 7 May 2019
Document identifier: NT3H2111/NT3H2211
Document number: 359935

life.augmented

M24LR64E-R

Dynamic NFC/RFID tag IC with 64-Kbit EEPROM, energy harvesting, I²C bus and ISO 15693 RF interface

Datasheet - production data



Features

- Belonging to ST25 family, which includes all NFC/RF ID tag and reader products from ST

I²C interface

- Two-wires I²C serial interface supports 400 kHz protocol
- Single supply voltage:
  - 1.8 V to 5.5 V
- Byte and Page Write (up to 4 bytes)
- Random and Sequential read modes
- Self-timed programming cycle
- Automatic address incrementing
- Enhanced ESD/latch-up protection
- I²C timeout

Contactless interface

- ISO 15693 and ISO 18000-3 mode 1 compatible
- 13.56 MHz ± 7 kHz carrier frequency
- To tag: 10% or 100% ASK modulation using 1/4 (26 Kbit/s) or 1/256 (1.6 Kbit/s) pulse position coding
- From tag: load modulation using Manchester coding with 423 kHz and 484 kHz subcarriers in low (6.6 kbit/s) or high (26 kbit/s) data rate mode. Supports the 53 kbit/s data rate with Fast commands
- Internal tuning capacitance: 27.5 pF
- 64-bit unique identifier (UID)
- Read Block & Write (32-bit blocks)

Digital output pin

- User configurable pin: RF write in progress or RF busy mode

Energy harvesting

- Analog pin for energy harvesting
- Four sink current configurable ranges

Temperature range

- From –40 to 85 °C

Memory

- 64-Kbit EEPROM organized into:
  - 8192 bytes in I²C mode
  - 2048 blocks of 32 bits in RF mode
- Write time
  - I²C: 5 ms (max.)
  - RF: 5.75 ms including the internal Verify time
- Write cycling endurance:
  - 1 million write cycles at 25 °C
  - 150 k write cycles at 85 °C
- More than 40-year data retention
- Multiple password protection in RF mode
- Single password protection in I²C mode

Package

- SO8 (ECOPACK2®)
- TSSOP8 (ECOPACK2®)
- UFDFPN8 (ECOPACK2®)

Contents

List of tables

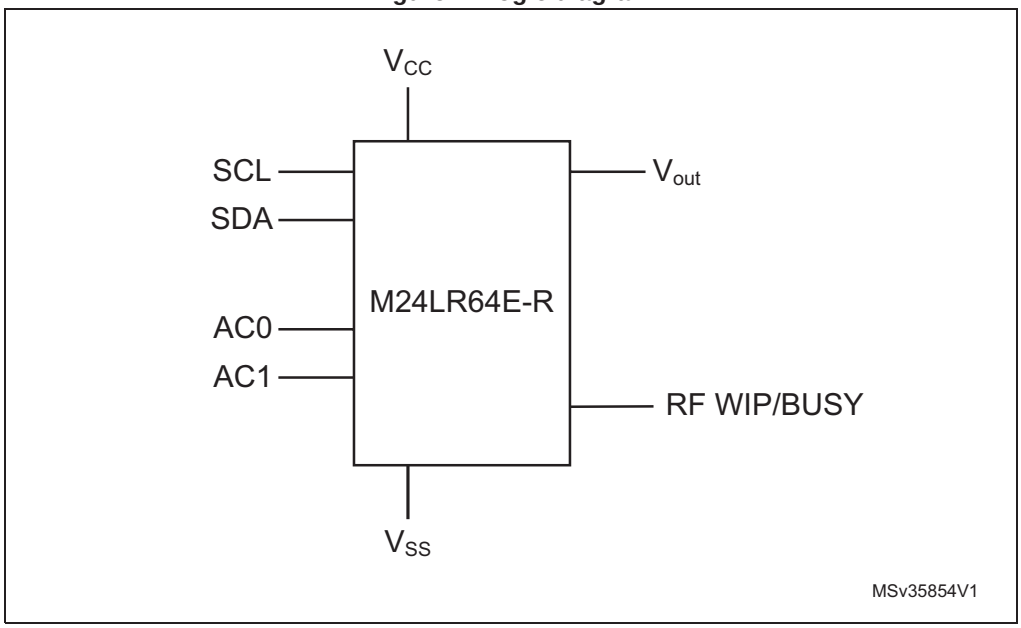
List of figures

1 Description

The M24LR64E-R device is a Dynamic NFC/RFID tag IC with a dual-interface, electrically erasable programmable memory (EEPROM). It features an I^2C interface and can be operated from a V_{CC} power supply. It is also a contactless memory powered by the received carrier electromagnetic wave. The M24LR64E-R is organized as 8192 × 8 bits in the I^2C mode and as 2048 × 32 bits in the ISO 15693 and ISO 18000-3 mode 1 RF mode.

The M24LR64E-R also features an energy harvesting analog output, as well as a user-configurable digital output pin toggling during either RF write in progress or RF busy mode.

Figure 1. Logic diagram



The I^2C uses a two-wire serial interface, comprising a bidirectional data line and a clock line. The devices carry a built-in 4-bit device type identifier code (1010) in accordance with the I^2C bus definition.

The device behaves as a slave in the I^2C protocol, with all memory operations synchronized by the serial clock. Read and Write operations are initiated by a Start condition, generated by the bus master. The Start condition is followed by a device select code and Read/$\overline{\text{Write}}$ bit ($\overline{\text{RW}}$) (as described in *Table 2*), terminated by an acknowledge bit.

When writing data to the memory, the device inserts an acknowledge bit during the 9^{th} bit time, following the bus master's 8-bit transmission. When data is read by the bus master, the bus master acknowledges the receipt of the data byte in the same way. Data transfers are terminated by a Stop condition after an Ack for Write, and after a NoAck for Read.

In the ISO15693/ISO18000-3 mode 1 RF mode, the M24LR64E-R is accessed via the 13.56 MHz carrier electromagnetic wave on which incoming data is demodulated from the received signal amplitude modulation (ASK: Amplitude Shift Keying). When connected to an antenna, the operating power is derived from the RF energy and no external power supply is required. The received ASK wave is 10% or 100% modulated with a data rate of 1.6 Kbit/s

using the 1 out of 256 pulse coding mode, or a data rate of 26 Kbit/s using the 1 out of 4 pulse coding mode.

Outgoing data is generated by the M24LR64E-R load variation using Manchester coding with one or two subcarrier frequencies at 423 kHz and 484 kHz. Data is transferred from the M24LR64E-R at 6.6 Kbit/s in low data rate mode and at 26 Kbit/s in high data rate mode. The M24LR64E-R supports the 53 Kbit/s fast mode in high data rate mode using one subcarrier frequency at 423 kHz.

The M24LR64E-R follows the ISO 15693 and ISO 18000-3 mode 1 recommendation for radio-frequency power and signal interface.

The M24LR64E-R provides an Energy harvesting mode on the analog output pin V_{out}. When the Energy harvesting mode is activated, the M24LR64E-R can output the excess energy coming from the RF field on the V_{out} analog pin. In case the RF field strength is insufficient or when the Energy harvesting mode is disabled, the analog output pin V_{out} goes into high-Z state and the Energy harvesting mode is automatically stopped.

The M24LR64E-R features a user configurable digital out pin RF WIP/BUSY that can be used to drive a microcontroller interrupt input pin (available only when the M24LR64E-R is correctly powered on the V_{CC} pin).

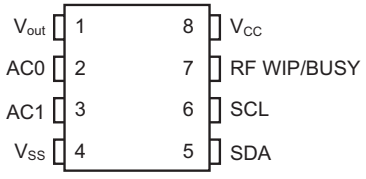
When configured in the RF write in progress mode (RF WIP mode), the RF WIP/BUSY pin is driven low for the entire duration of the RF internal write operation. When configured in the RF busy mode (RF BUSY mode), the RF WIP/BUSY pin is driven low for the entire duration of the RF command progress.

The RF WIP/BUSY pin is an open drain output and must be connected to a pull-up resistor.

Table 1. Signal names

Signal name	Function	Direction
V_{out}	Energy harvesting Output	Analog output
SDA	Serial Data	I/O
SCL	Serial Clock	Input
AC0, AC1	Antenna coils	I/O
V_{CC}	Supply voltage	-
RF WIP/BUSY	Digital signal	Digital output
V_{SS}	Ground	-

Figure 2. 8-pin package connections



1. See *Section 31* for package dimensions, and how to identify pin 1.

2 Signal descriptions

2.1 Serial clock (SCL)

This input signal is used to strobe all data in and out of the device. In applications where this signal is used by slave devices to synchronize the bus to a slower clock, the bus master must have an open drain output, and a pull-up resistor must be connected from Serial Clock (SCL) to V_{CC}. (*Figure 3* indicates how the value of the pull-up resistor can be calculated). In most applications, though, this method of synchronization is not employed, and so the pull-up resistor is not necessary, provided that the bus master has a push-pull (rather than open drain) output.

2.2 Serial data (SDA)

This bidirectional signal is used to transfer data in or out of the device. It is an open drain output that may be wire-OR'ed with other open drain or open collector signals on the bus. A pull-up resistor must be connected from Serial Data (SDA) to V_{CC}. (*Figure 3* indicates how the value of the pull-up resistor can be calculated).

2.3 RF Write in progress / RF Busy (RF WIP/BUSY)

This configurable output signal is used either to indicate that the M24LR64E-R is executing an internal write cycle from the RF channel or that an RF command is in progress. RF WIP and signals are available only when the M24LR64E-R is powered by the Vcc pin. It is an open drain output and a pull-up resistor must be connected from RF WIP/BUSY to V_{CC}.

2.4 Energy harvesting analog output (V_{out})

This analog output pin is used to deliver the analog voltage V_{out} available when the Energy harvesting mode is enabled and the RF field strength is sufficient. When the Energy harvesting mode is disabled or the RF field strength is not sufficient, the energy harvesting analog voltage output Vout is in High-Z state.

2.5 Antenna coil (AC0, AC1)

These inputs are used to connect the device to an external coil exclusively. It is advised not to connect any other DC or AC path to AC0 or AC1.

When correctly tuned, the coil is used to power and access the device using the ISO 15693 and ISO 18000-3 mode 1 protocols.

2.5.1 Device reset in RF mode

To ensure a proper reset of the RF circuitry, the RF field must be turned off (100% modulation) for a minimum t_{RF_OFF} period of time.

2.6 V_{SS} ground

V_{SS} is the reference for the V_{CC} supply voltage and V_{out} analog output voltage.

2.7 Supply voltage (V_{CC})

This pin can be connected to an external DC supply voltage.

Note: An internal voltage regulator allows the external voltage applied on V_{CC} to supply the M24LR64E-R, while preventing the internal power supply (rectified RF waveforms) to output a DC voltage on the V_{CC} pin.

2.7.1 Operating supply voltage V_{CC}

Prior to selecting the memory and issuing instructions to it, a valid and stable V_{CC} voltage within the specified [V_{CC}(min), V_{CC}(max)] range must be applied (see *Table 119*). To maintain a stable DC supply voltage, it is recommended to decouple the V_{CC} line with a suitable capacitor (usually around 10 nF) close to the V_{CC}/V_{SS} package pins.

This voltage must remain stable and valid until the end of the transmission of the instruction and, for a Write instruction, until the completion of the internal I²C write cycle (t_W).

2.7.2 Power-up conditions

When the power supply is turned on, V_{CC} rises from V_{SS} to V_{CC}. The V_{CC} rise time must not vary faster than 1V/µs.

2.7.3 Device reset in I²C mode

In order to prevent inadvertent write operations during power-up, a power-on reset (POR) circuit is included. At power-up (continuous rise of V_{CC}), the device does not respond to any I²C instruction until V_{CC} has reached the power-on reset threshold voltage (this threshold is lower than the minimum V_{CC} operating voltage defined in *Table 119*). When V_{CC} passes over the POR threshold, the device is reset and enters the Standby power mode. However, the device must not be accessed until V_{CC} has reached a valid and stable V_{CC} voltage within the specified [V_{CC}(min), V_{CC}(max)] range.

In a similar way, during power-down (continuous decrease in V_{CC}), as soon as V_{CC} drops below the power-on reset threshold voltage, the device stops responding to any instruction sent to it.

2.7.4 Power-down conditions

During power-down (continuous decay of V_{CC}), the device must be in Standby power mode (mode reached after decoding a Stop condition, assuming that there is no internal write cycle in progress).

Figure 3. I²C Fast mode (f_C = 400 kHz): maximum R_{bus} value versus bus parasitic capacitance (C_{bus})

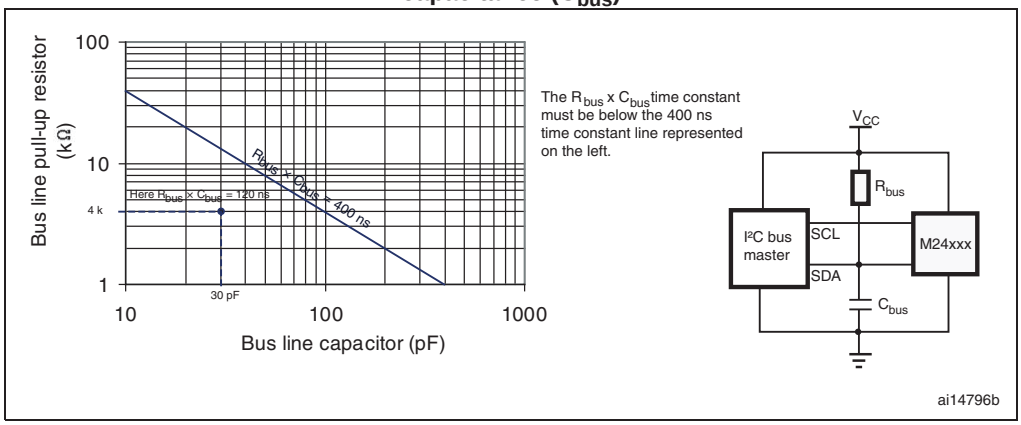


Figure 4. I²C bus protocol

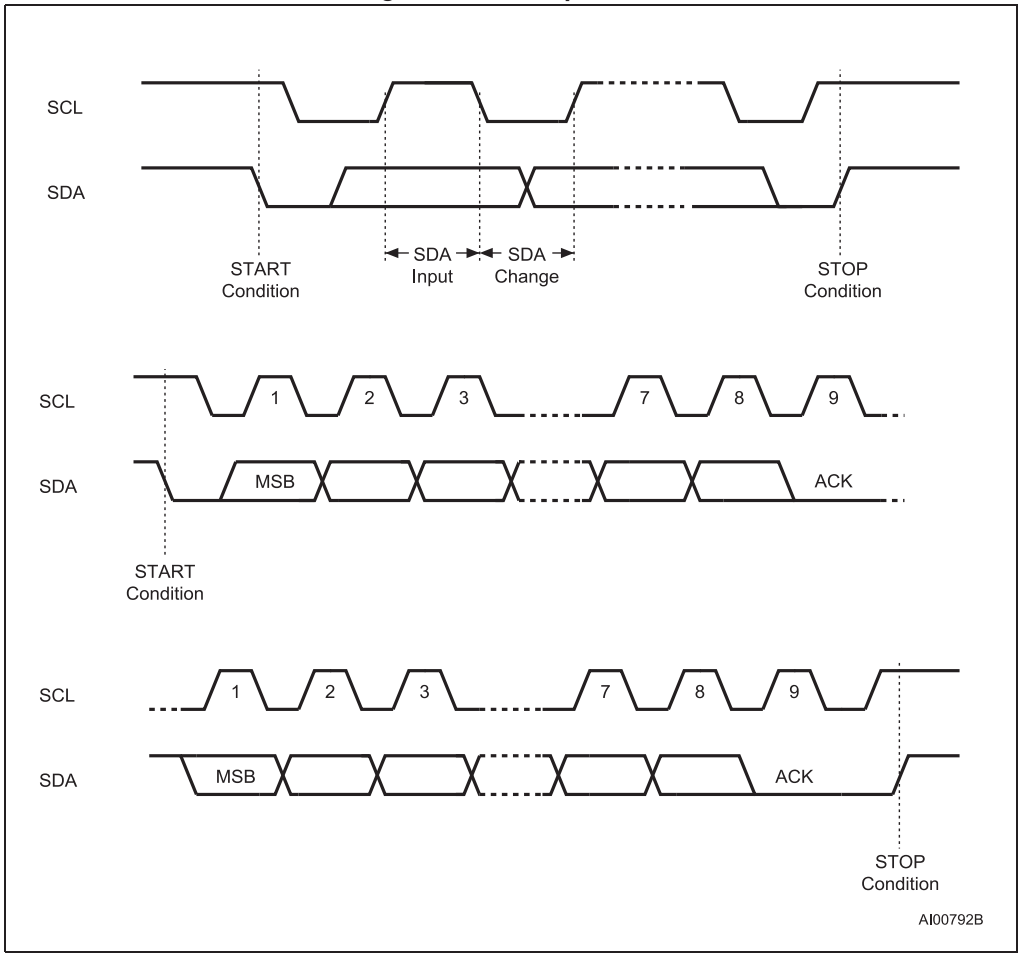


Table 2. Device select code

-	Device type identifier(1)				Chip Enable address			RW
	b7	b6	b5	b4	b3	b2	b1	b0
Device select code	1	0	1	0	E2(2)	1	1	RW

1. The most significant bit, b7, is sent first.
2. E2 is not connected to any external pin. It is however used to address the M24LR64E-R as described in *Section 3* and *Section 4*.

Table 3. Address most significant byte

b15	b14	b13	b12	b11	b10	b9	b8

Table 4. Address least significant byte

b7	b6	b5	b4	b3	b2	b1	b0

3 User memory organization

The M24LR64E-R is divided into 64 sectors of 32 blocks of 32 bits, as shown in *Table 5*. *Figure 6* shows the memory sector organization. Each sector can be individually read- and/or write-protected using a specific password command. Read and write operations are possible if the addressed data is not in a protected sector.

The M24LR64E-R also has a 64-bit block that is used to store the 64-bit unique identifier (UID). The UID is compliant with the ISO 15963 description, and its value is used during the anticollision sequence (Inventory). This block is not accessible by the user in RF device operation and its value is written by ST on the production line.

The M24LR64E-R includes an AFI register that stores the application family identifier, and a DSFID register that stores the data storage family identifier used in the anticollision algorithm.

The M24LR64E-R has four 32-bit blocks that store an I^2C password plus three RF password codes.

Figure 5. Circuit diagram

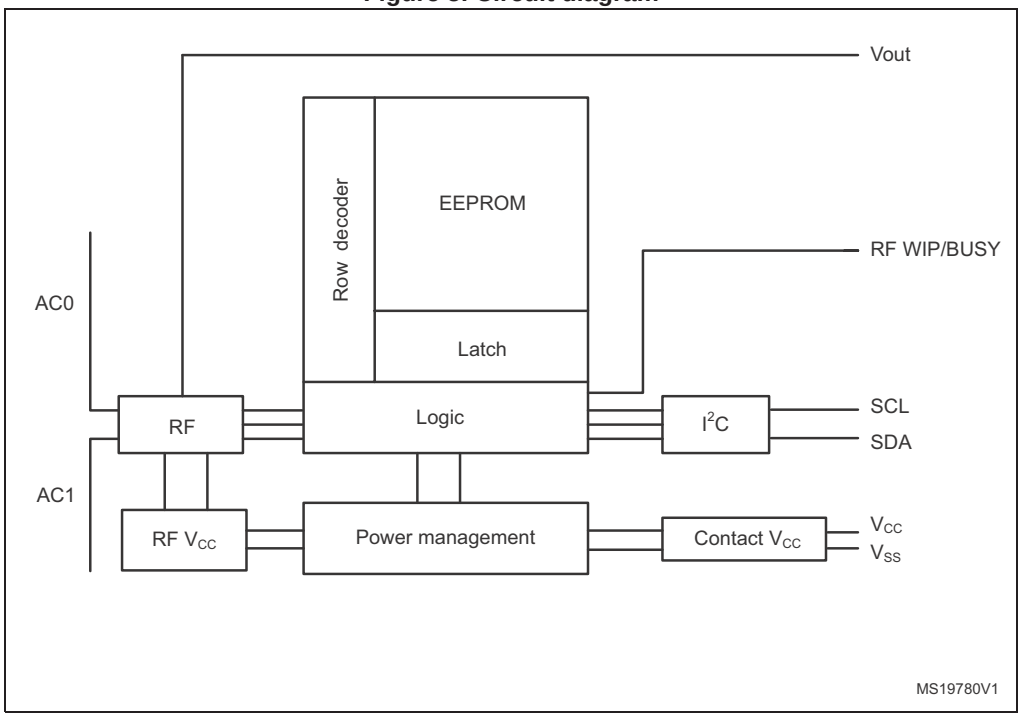
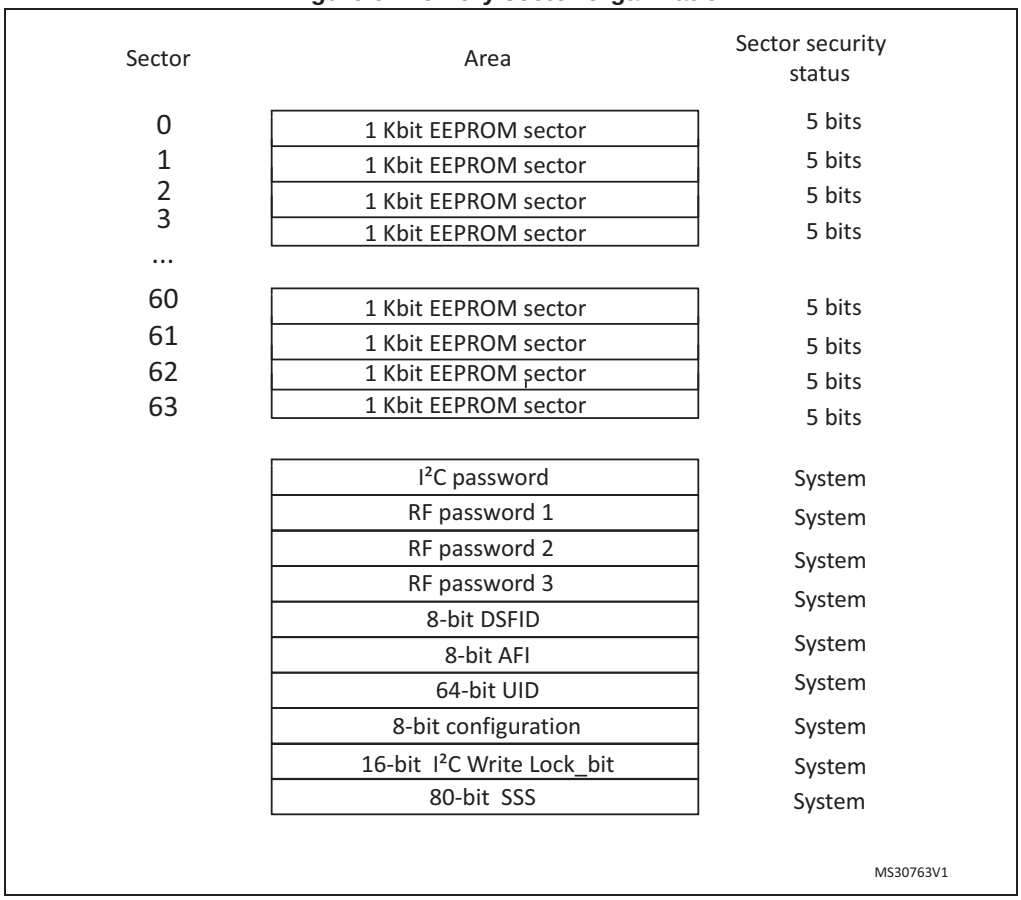


Figure 6. Memory sector organization



Sector details

The M24LR64E-R user memory is divided into 64 sectors. Each sector contains 1024 bits. The protection scheme is described in *Section 4: System memory area*.

In RF mode, a sector provides 32 blocks of 32 bits. Each read and write access is done by block. Read and write block accesses are controlled by a Sector Security Status byte that defines the access rights to the 32 blocks contained in the sector. If the sector is not protected, a Write command updates the complete 32 bits of the selected block.

In I^2C mode, a sector provides 128 bytes that can be individually accessed in Read and Write modes. When protected by the corresponding I2C_Write_Lock bit, the entire sector is write-protected. To access the user memory, the device select code used for any I^2C command must have the E2 Chip Enable address at 0.

Table 5. Sector details

Sector number	RF block address	I^2C byte address	Bits [31:24]	Bits [23:16]	Bits [15:8]	Bits [7:0]
0	0	0	user	user	user	user
	1	4	user	user	user	user
	2	8	user	user	user	user
	3	12	user	user	user	user
	4	16	user	user	user	user
	5	20	user	user	user	user
	6	24	user	user	user	user
	7	28	user	user	user	user
	8	32	user	user	user	user
	9	36	user	user	user	user
	10	40	user	user	user	user
	11	44	user	user	user	user
	12	48	user	user	user	user
	13	52	user	user	user	user
	14	56	user	user	user	user
	15	60	user	user	user	user
	16	64	user	user	user	user
	17	68	user	user	user	user
	18	72	user	user	user	user
	19	76	user	user	user	user
	20	80	user	user	user	user
	21	84	user	user	user	user
	22	88	user	user	user	user
	23	92	user	user	user	user
	24	96	user	user	user	user
	25	100	user	user	user	user
	26	104	user	user	user	user
	27	108	user	user	user	user
	28	112	user	user	user	user
	29	116	user	user	user	user
	30	120	user	user	user	user
	31	124	user	user	user	user

Table 5. Sector details (continued)

Sector number	RF block address	I^2C byte address	Bits [31:24]	Bits [23:16]	Bits [15:8]	Bits [7:0]
1	32	128	user	user	user	user
	33	132	user	user	user	user
	34	136	user	user	user	user
	35	140	user	user	user	user
	36	144	user	user	user	user
	37	148	user	user	user	user
	38	152	user	user	user	user
	39	156	user	user	user	user
	⋮	⋮	⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮	⋮	⋮	⋮

Table 5. Sector details (continued)

Sector number	RF block address	I^2C byte address	Bits [31:24]	Bits [23:16]	Bits [15:8]	Bits [7:0]
63	2016	8064	user	user	user	user
	2017	8068	user	user	user	user
	2018	8072	user	user	user	user
	2019	8076	user	user	user	user
	2020	8080	user	user	user	user
	2021	8084	user	user	user	user
	2022	8088	user	user	user	user
	2023	8092	user	user	user	user
	2024	8096	user	user	user	user
	2025	8100	user	user	user	user
	2026	8104	user	user	user	user
	2027	8108	user	user	user	user
	2028	8112	user	user	user	user
	2029	8116	user	user	user	user
	2030	8120	user	user	user	user
	2031	8124	user	user	user	user
	2032	8128	user	user	user	user
	2033	8132	user	user	user	user
	2034	8136	user	user	user	user
	2035	8140	user	user	user	user
	2036	8144	user	user	user	user
	2037	8148	user	user	user	user
	2038	8152	user	user	user	user
	2039	8156	user	user	user	user
	2040	8160	user	user	user	user
	2041	8164	user	user	user	user
	2042	8168	user	user	user	user
	2043	8172	user	user	user	user
	2044	8176	user	user	user	user
	2045	8180	user	user	user	user
	2046	8184	user	user	user	user
	2047	8188	user	user	user	user

4 System memory area

4.1 M24LR64E-R block security in RF mode

The M24LR64E-R provides a special protection mechanism based on passwords. In RF mode, each memory sector of the M24LR64E-R can be individually protected by one out of three available passwords, and each sector can also have Read/Write access conditions set.

Each memory sector of the M24LR64E-R is assigned with a Sector security status byte including a Sector Lock bit, two Password Control bits and two Read/Write protection bits, as shown in *Table 7*.

Table 6 describes the organization of the Sector security status byte, which can be read using the Read Single Block and Read Multiple Block commands with the Option_flag set to 1.

On delivery, the default value of the SSS bytes is set to 00h.

Table 6. Sector security status byte area

I^2C byte address		Bits [31:24]	Bits [23:16]	Bits [15:8]	Bits [7:0]
E2 = 1	0	SSS 3	SSS 2	SSS 1	SSS 0
E2 = 1	4	SSS 7	SSS 6	SSS 5	SSS 4
E2 = 1	8	SSS 11	SSS 10	SSS 9	SSS 8
E2 = 1	12	SSS 15	SSS 14	SSS 13	SSS 12
E2 = 1	16	SSS 19	SSS 18	SSS 17	SSS 16
E2 = 1	20	SSS 23	SSS 22	SSS 21	SSS 20
E2 = 1	24	SSS 27	SSS 26	SSS 25	SSS 24
E2 = 1	28	SSS 31	SSS 30	SSS 29	SSS 28
E2 = 1	32	SSS 35	SSS 34	SSS 33	SSS 32
E2 = 1	36	SSS 39	SSS 38	SSS 37	SSS 36
E2 = 1	40	SSS 43	SSS 42	SSS 41	SSS 40
E2 = 1	44	SSS 47	SSS 46	SSS 45	SSS 44
E2 = 1	48	SSS 51	SSS 50	SSS 49	SSS 48
E2 = 1	52	SSS 55	SSS 54	SSS 53	SSS 52
E2 = 1	56	SSS 59	SSS 58	SSS 57	SSS 56
E2 = 1	60	SSS 63	SSS 62	SSS 61	SSS 60

Table 7. Sector security status byte organization

b_7	b_6	b_5	b_4	b_3	b_2	b_1	b_0
0	0	0	Password control bits		Read / Write protection bits		Sector Lock

When the Sector Lock bit is set to 1, for instance by issuing a Lock-sector command, the two Read/Write protection bits (b_1, b_2) are used to set the Read/Write access of the sector as described in *Table 8*.

Table 8. Read/Write protection bit setting

Sector Lock	b_2, b_1	Sector access when password presented		Sector access when password not presented	
0	xx	Read	Write	Read	Write
1	00	Read	Write	Read	No Write
1	01	Read	Write	Read	Write
1	10	Read	Write	No Read	No Write
1	11	Read	No Write	No Read	No Write

The next two bits of the Sector security status byte (b_3, b_4) are the password control bits. The value of these two bits is used to link a password to the sector, as defined in *Table 9*.

Table 9. Password control bits

b_4, b_3	Password
00	The sector is not protected by a password.
01	The sector is protected by password 1.
10	The sector is protected by password 2.
11	The sector is protected by password 3.

The M24LR64E-R password protection is organized around a dedicated set of commands, plus a system area of three password blocks where the password values are stored. This system area is described in *Table 10*.

Table 10. Password system area

Add	Password
1	Password 1
2	Password 2
3	Password 3

The dedicated commands for protection in RF mode are:

- Write-sector password:

  The Write-sector password command is used to write a 32-bit block into the password system area. This command must be used to update password values. After the write cycle, the new password value is automatically activated. It is possible to modify a password value after issuing a valid Present-sector password command. On delivery, the three default password values are set to 0000 0000h and are activated.

- Lock-sector:

  The Lock-sector command is used to set the sector security status byte of the selected sector. Bits b_4 to b_1 of the sector security status byte are affected by the Lock-sector

command. The sector lock bit, b_0, is set to 1 automatically. After issuing a Lock-sector command, the protection settings of the selected sector are activated. The protection of a locked block cannot be changed in RF mode. A Lock-sector command sent to a locked sector returns an error code.

- Present-sector password:

  The Present-sector password command is used to present one of the three passwords to the M24LR64E-R in order to modify the access rights of all the memory sectors linked to that password (*Table 8*) including the password itself. If the presented password is correct, the access rights remain activated until the tag is powered off or until a new Present-sector password command is issued. If the presented password value is not correct, all the access rights of all the memory sectors are deactivated.

- Sector security status byte area access conditions in I^2C mode:

  In I^2C mode, read access to the sector security status byte area is always allowed. Write access depends on the correct presentation of the I^2C password (see *Section 5.16.1: I^2C present password command description*).

  To access the Sector security status byte area, the device select code used for any I^2C command must have the E2 Chip Enable address at 1.

  An I^2C write access to a sector security status byte re-initializes the RF access condition to the given memory sector.

4.1.1 Example of the M24LR64E-R security protection in RF mode

Table 11 and *Table 12* show the sector security protections before and after a valid Present-sector password command. *Table 11* shows the sector access rights of an M24LR64E-R after power-up. After a valid Present-sector password command with password 1, the memory sector access is changed as shown in *Table 12*.

Table 11. M24LR64E-R sector security protection after power-up

Sector address	Sector features			Sector security status byte					
				$b_7b_6b_5$	b_4	b_3	b_2	b_1	b_0
0	Protection: standard	Read	No Write	xxx	0	0	0	0	1
1	Protection: password 1	Read	No Write	xxx	0	1	0	0	1
2	Protection: password 1	Read	Write	xxx	0	1	0	1	1
3	Protection: password 1	No Read	No Write	xxx	0	1	1	0	1
4	Protection: password 1	No Read	No Write	xxx	0	1	1	1	1

Table 12. M24LR64E-R sector security protection after a valid presentation of password 1

Sector address	Sector features			Sector security status byte					
				$b_7b_6b_5$	b_4	b_3	b_2	b_1	b_0
0	Protection: standard	Read	No Write	xxx	0	0	0	0	1
1	Protection: password 1	Read	Write	xxx	0	1	0	0	1
2	Protection: password 1	Read	Write	xxx	0	1	0	1	1

Table 12. M24LR64E-R sector security protection after a valid presentation of password 1 (continued)

Sector address	Sector features			Sector security status byte					
				$b_7b_6b_5$	b_4	b_3	b_2	b_1	b_0
3	Protection: password 1	Read	Write	xxx	0	1	1	0	1
4	Protection: password 1	Read	No Write	xxx	0	1	1	1	1

4.2 M24LR64E-R block security in I²C mode (I2C_Write_Lock bit area)

In the I^2C mode only, it is possible to protect individual sectors against Write operations. This feature is controlled by the I2C_Write_Lock bits stored in the 8 bytes of the I2C_Write_Lock bit area. I2C_Write_Lock bit area starts from location 8192 (see *Table 13*). To access the I2C_Write_Lock bit area, the device select code used for any I^2C command must have the E2 Chip Enable address at 1.

Using these 16 bits, it is possible to write-protect all the 64 sectors of the M24LR64E-R memory. Each bit controls the I^2C write access to a specific sector as shown in *Table 13*. It is always possible to unprotect a sector in the I^2C mode. When an I2C_Write_Lock bit is reset to 0, the corresponding sector is unprotected. When the bit is set to 1, the corresponding sector is write-protected.

In I^2C mode, read access to the I2C_Write_Lock bit area is always allowed. Write access depends on the correct presentation of the I^2C password.

On delivery, the default value of the eight bytes of the I2C_Write_Lock bit area is reset to 00h.

Table 13. I2C_Write_Lock bit

I^2C byte address		Bits [31:24]	Bits [23:16]	Bits [15:8]	Bits [7:0]
E2 = 1	2048	sectors 31-24	sectors 23-16	sectors 15-8	sectors 7-0
E2 = 1	2052	sectors 63-56	sectors 55-48	sectors 47-40	sectors 39-32

4.3 Configuration byte and Control register

The M24LR64E-R offers an 8-bit non-volatile Configuration byte located at I²C location 2320 of the system area used to store the RF WIP/BUSY pin and the energy harvesting configuration (see *Table 14*).

The M24LR64E-R also offers an 8-bit volatile Control register located at I²C location 2336 of the system area used to store the energy harvesting enable bit as well as a FIELD_ON bit indicator (see *Table 15*).

4.3.1 RF WIP/BUSY pin configuration

The M24LR64E-R features a configurable open drain output RF WIP/BUSY pin used to provide RF activity information to an external device.

The RF WIP/BUSY pin functionality depends on the value of bit 3 of the Configuration byte.

- **RF busy mode**

When bit 3 of the Configuration byte is set to 0, the RF WIP/BUSY pin is configured in RF busy mode.

The purpose of this mode is to indicate to the I²C bus master whether the M24LR64E-R is busy in RF mode or not.

In this mode, the RF WIP/BUSY pin is tied to 0 from the RF command Start Of Frame (SOF) until the end of the command execution.

If a bad RF command is received, the RF WIP/BUSY pin is tied to 0 from the RF command SOF until the reception of the RF command CRC. Otherwise, the RF WIP/BUSY pin is in high-Z state.

When tied to 0, the RF WIP/BUSY signal returns to High-Z state if the RF field is cut-off.

During the execution of I²C commands, the RF WIP/BUSY pin remains in high-Z state.

- **RF Write in progress**

When bit 3 of the Configuration byte is set to 1, the RF WIP/BUSY pin is configured in RF Write in progress mode.

The purpose of this mode is to indicate to the I²C bus master that some data has been changed in RF mode.

In this mode, the RF WIP/BUSY pin is tied to 0 for the duration of an internal write operation (i.e. between the end of a valid RF write command and the beginning of the RF answer).

During the execution of I²C write operations, the RF WIP/BUSY pin remains in high-Z state.

4.3.2 Energy harvesting configuration

The M24LR64E-R features an Energy harvesting mode on the V_{out} analog output.

The general purpose of the Energy harvesting mode is to deliver a part of the non-necessary RF power received by the M24LR64E-R on the AC0-AC1 RF input in order to supply an external device. The current consumption on the analog voltage output V_{out} is limited to ensure that the M24LR64E-R is correctly supplied during the powering of the external device.

When the Energy harvesting mode is enabled and the power delivered on the AC0-AC1 RF input exceeds the minimum required $P_{AC0\text{-}AC1\_min}$, the M24LR64E-R is able to deliver a limited and unregulated voltage on the V_{out} pin, assuming the current consumption on the V_{out} does not exceed the I_{sink_max} maximum value.

If one of the conditions above is not met, the analog voltage output pin V_{out} is set in High-Z state.

For robust applications using the Energy harvesting mode, four current fan-out levels can be chosen.

- **V_{out} sink current configuration**

The sink current level is chosen by programming EH_cfg1 and EH_cfg0 into the Configuration byte (see *Table 14*).

The minimum power level required on AC0-AC1 RF input $P_{AC0\text{-}AC1\_min}$, the delivered voltage V_{out}, as well as the maximum current consumption I_{sink_max} on the V_{out} pin corresponding to the <EH_cfg1,EH_cfg0> bit values are described in *Table 127*.

Table 14. Configuration byte

I²C byte address		Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	BIT 1	BIT 0
E2=1	2320	X(1)	X(1)	X(1)	X(1)	RF WIP/BUSY	EH_mode	EH_cfg1	EH_cfg0

1. Bit 7 to bit 4 are don't care bits.

- **Energy harvesting enable control**

Delivery of Energy harvesting analog output voltage on the V_{out} pin depends on the value of the EH_enable bit of the volatile Control register (see *Table 15*).

Table 15. Control register

I²C byte address		Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	BIT 1	BIT 0
E2=1	2336	T-Prog(1)	0(1)	0(1)	0(1)	0(1)	0(1)	FIELD_ON(1)	EH_enable

1. Bit 7 to bit 1 are read-only bits.

  - When set to 1, the EH_enable bit enables the Energy harvesting mode, meaning that the V_{out} analog output signal is delivered when the $P_{AC0\text{-}AC1\_min}$ and I_{sink_max} conditions corresponding to the chosen sink current configuration bit are met (see *Table 127*).
  - When set to 0, the EH_enable bit disables the Energy harvesting mode and the analog output V_{out} remains in High-Z state.
  - The T_Prog flag indicates a correct duration of the I²C write time (tw). This bit is reset to 0 after POR and at the beginning of each writing cycle; it is set to 1 only after a correct completion of the writing cycle.

- **Energy harvesting default mode control**

At power-up, in I²C or RF mode, the EH_enable bit is updated according to the value of the EH_mode bit stored in the non-volatile Configuration byte (see *Table 16*). In other words, the EH_mode bit is used to configure whether the Energy harvesting mode is enabled or not by default.

Table 16. EH_enable bit value after power-up

EH_mode value	EH_enable after power-up	Energy harvesting after power-up
0	1	enabled
1	0	disabled

4.3.3 FIELD_ON indicator bit

The FIELD_ON indicator bit located as bit 1 of the Control register is a read-only bit used to indicate when the RF power level delivered to the M24LR64E-R is sufficient to execute RF commands.

- When FIELD_ON = 0, the M24LR64E-R is not able to execute any RF commands.
- When FIELD_ON =1, the M24LR64E-R is able to execute any RF commands.

Note: During read access to the Control register in RF mode, the FIELD_ON bit is always read at 1.

4.3.4 Configuration byte access in I²C and RF modes

In I²C mode, read and write accesses to the non-volatile Configuration byte are always allowed. To access the Configuration byte, the device select code used for any I²C command must have the E2 Chip enable address at 1.

The dedicated commands to access the Configuration byte in RF mode are:

- Read configuration byte command (ReadCfg):
  - The ReadCfg command is used to read the eight bits of the Configuration byte.
- Write energy harvesting configuration command (WriteEHCfg):
  - The WriteEHCfg command is used to write the EH_mode, EH_cfg1 and EH_cfg0 bits into the Configuration byte.
- Write RF WIP/BUSY pin configuration command (WriteDOCfg):
  - The WriteDOCfg command is used to write the RF WIP/BUSY bit into the Configuration byte.

After any write access to the Configuration byte, the new configuration is automatically applied.

4.3.5 Control register access in I²C or RF mode

In I²C mode, read and write accesses to the volatile Control register are always allowed. To access the Control register, the device select code used for any I²C command must have the E2 Chip enable address at 1.

The dedicated commands to access the Control register in RF mode are:

- Check energy harvesting enable bit command (CheckEHEn):
  - The CheckEHEn command is used to read the eight bits of the Control register. When it is run, the FIELD_ON bit is always read at 1.
- Set/reset energy harvesting enable bit command (SetRstEHEn):
  - The SetRstEHEn command is used to set or reset the value of the EH_enable bit into the Control register.

4.4 ISO 15693 system parameters

The M24LR64E-R provides the system area required by the ISO 15693 RF protocol, as shown in *Table 17*.

The first 32-bit block starting from I^2C address 2304 stores the I^2C password. This password is used to activate/deactivate the write protection of the protected sector in I^2C

mode. At power-on, all user memory sectors protected by the I2C_Write_Lock bits can be read but cannot be modified. To remove the write protection, it is necessary to use the I^2C present password described in *Figure 12*. When the password is correctly presented — that is, when all the presented bits correspond to the stored ones — it is also possible to modify the I^2C password using the I^2C write password command described in *Figure 13*.

The next three 32-bit blocks store the three RF passwords. These passwords are neither read- nor write- accessible in the I^2C mode.

The next byte stores the Configuration byte, at I²C location 2320. This Control register is used to store the three energy harvesting configuration bits and the RF WIP/BUSY configuration bit.

The next two bytes are used to store the AFI, at I^2C location 2322, and the DSFID, at I^2C location 2323. These two values are used during the RF inventory sequence. They are read-only in the I^2C mode.

The next eight bytes, starting from location 2324, store the 64-bit UID programmed by ST on the production line. Bytes at I^2C locations 2332 to 2335 store the IC Ref and the Mem_Size data used by the RF Get_System_Info command. The UID, Mem_Size and IC ref values are read-only data.

Table 17. System parameter sector

I^2C byte address		Bits [31:24]	Bits [23:16]	Bits [15:8]	Bits [7:0]
E2 = 1	2304	I^2C password(1)			
E2 = 1	2308	RF password 1(1)			
E2 = 1	2312	RF password 2(1)			
E2 = 1	2316	RF password 3(1)			
E2 = 1	2320	DSFID (FFh)	AFI (00h)	ST reserved (Exh)(2)	Configuration byte (F4h)
E2 = 1	2324	UID	UID	UID	UID
E2 = 1	2328	UID (E0h)	UID (02h)	UID	UID
E2 = 1	2332	Mem_Size (03 07FFh)			IC Ref (5Eh)
E2 = 1	2336	-	-	-	Prog. completion and Energy harvesting status(3)

1. Delivery state: I^2C password = 0000 0000h, RF password = 0000 0000h, Configuration byte = F4h
2. The product revision is the Most significant nibble of the byte located at address 0x911 (2321 d) in the system area (Device select code E2 =1). From DS rev4, the product revision value is 0xE. The Least significant nibble is ST reserved.
3. Address system 2336 (920h, E2=1) is the control register.
   Bit 7 is T_Prog (refer to *Table 15: Control register*). When accessed in RF, this bit is not significant and set to 0.
   Bits 2-6 are RFU and set to 0.
   Bit 1 is FIELD_ON (refer to *Table 15: Control register*).
   Bit 0 is EH_enable (refer to *Table 15: Control register*).

5 I²C device operation

The device supports the I²C protocol. This is summarized in *Figure 4*. Any device that sends data to the bus is defined as a transmitter, and any device that reads data is defined as a receiver. The device that controls the data transfer is known as the bus master, and the other as the slave device. A data transfer can only be initiated by the bus master, which also provides the serial clock for synchronization. The M24LR64E-R device is a slave in all communications.

5.1 Start condition

Start is identified by a falling edge of serial data (SDA) while the serial clock (SCL) is stable in the high state. A Start condition must precede any data transfer command. The device continuously monitors (except during a write cycle) the SDA and the SCL for a Start condition, and does not respond unless one is given.

5.2 Stop condition

Stop is identified by a rising edge of serial data (SDA) while the serial clock (SCL) is stable and driven high. A Stop condition terminates communication between the device and the bus master. A Read command that is followed by NoAck can be followed by a Stop condition to force the device into the Standby mode. A Stop condition at the end of a Write command triggers the internal write cycle.

5.3 Acknowledge bit (Ack)

The acknowledge bit is used to indicate a successful byte transfer. The bus transmitter, whether a bus master or a slave device, releases the serial data (SDA) after sending eight bits of data. During the 9th clock pulse period, the receiver pulls the SDA low to acknowledge the receipt of the eight data bits.

5.4 Data input

During data input, the device samples serial data (SDA) on the rising edge of the serial clock (SCL). For correct device operation, the SDA must be stable during the rising edge of the SCL, and the SDA signal must change *only* when the SCL is driven low.

5.5 I²C timeout

During the execution of an I²C operation, RF communications are not possible.

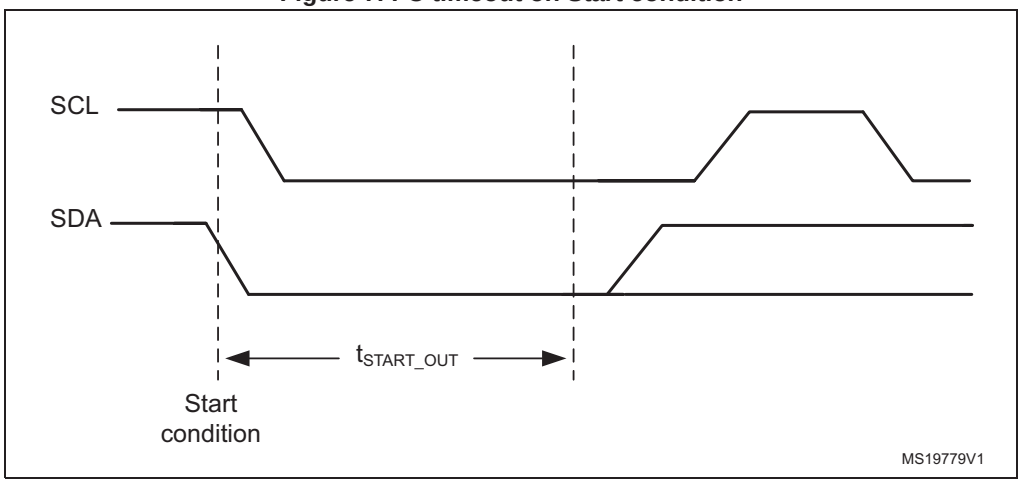
To prevent RF communication freezing due to inadvertent unterminated instructions sent to the I²C bus, the M24LR64E-R features a timeout mechanism that automatically resets the I²C logic block.

5.5.1 I²C timeout on Start condition

I²C communication with the M24LR64E-R starts with a valid Start condition, followed by a device select code.

If the delay between the Start condition and the following rising edge of the Serial Clock (SCL) that samples the most significant of the Device Select exceeds the t_{START_OUT} time (see *Table 123*), the I²C logic block is reset and further incoming data transfer is ignored until the next valid Start condition.

Figure 7. I²C timeout on Start condition



5.5.2 I²C timeout on clock period

During data transfer on the I²C bus, if the serial clock pulse width high (t_{CHCL}) or serial clock pulse width low (t_{CLCH}) exceeds the maximum value specified in *Table 123*, the I²C logic block is reset and any further incoming data transfer is ignored until the next valid Start condition.

5.6 Memory addressing

To start a communication between the bus master and the slave device, the bus master must initiate a Start condition. Following this, the bus master sends the device select code, shown in *Table 2* (on Serial Data (SDA), the most significant bit first).

The device select code consists of a 4-bit device type identifier and a 3-bit Chip Enable "Address" (E2,1,1). To address the memory array, the 4-bit device type identifier is 1010b. Refer to *Table 2*.

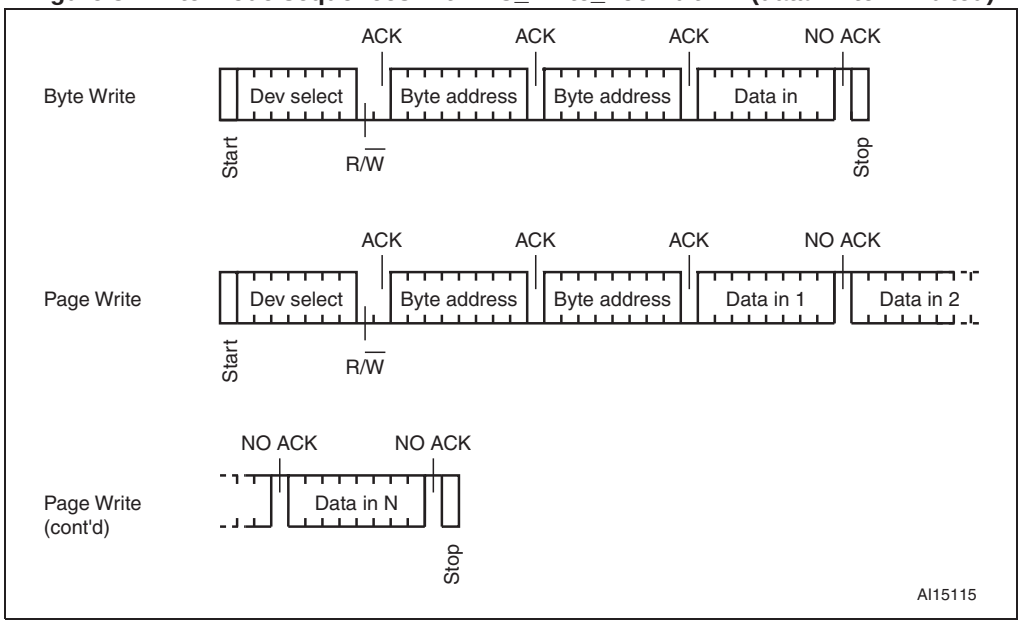
The eighth bit is the Read/$\overline{\text{Write}}$ bit ($\overline{\text{RW}}$). It is set to 1 for Read and to 0 for Write operations.

If a match occurs on the device select code, the corresponding device gives an acknowledgment on serial data (SDA) during the ninth bit time. If the device does not match the device select code, it deselects itself from the bus, and goes into Standby mode.

Table 18. Operating modes

Mode	RW bit	Bytes	Initial sequence
Current address read	1	1	Start, device select, RW = 1
Random address read	0	1	Start, device select, RW = 0, address
	1		reStart, device select, RW = 1
Sequential read	1	≥ 1	Similar to current or random address read
Byte write	0	1	Start, device select, RW = 0
Page write	0	≤ 4 bytes	Start, device select, RW = 0

Figure 8. Write mode sequences with I2C_Write_Lock bit = 1 (data write inhibited)



5.7 Write operations

Following a Start condition, the bus master sends a device select code with the Read/Write bit (RW) reset to 0. The device acknowledges this, as shown in *Figure 8*, and waits for two address bytes. The device responds to each address byte with an acknowledge bit, and then waits for the data byte.

Writing to the memory may be inhibited if the I2C_Write_Lock bit = 1. A Write instruction issued with the I2C_Write_Lock bit = 1 and with no I2C_Password presented does not modify the memory contents, and the accompanying data bytes are *not* acknowledged, as shown in *Figure 8*.

Each data byte in the memory has a 16-bit (two-byte wide) address. The most significant byte (*Table 3*) is sent first, followed by the least significant byte (*Table 4*). Bits b15 to b0 form the address of the byte in memory.

When the bus master generates a Stop condition immediately after the Ack bit (in the tenth-bit time slot), either at the end of a byte write or a page write, the internal write cycle is triggered. A Stop condition at any other time slot does not trigger the internal write cycle.

After the Stop condition, the delay t_W, and the successful completion of a Write operation, the device's internal address counter is incremented automatically, to point to the next byte address after the last one that was modified.

During the internal write cycle, the serial data (SDA) signal is disabled internally, and the device does not respond to any requests.

5.8 Byte write

After the device select code and the address bytes, the bus master sends one data byte. If the addressed location is write-protected by the I2C_Write_Lock bit (= 1), the device replies with NoAck, and the location is not modified. If the addressed location is not write-protected, the device replies with Ack. The bus master terminates the transfer by generating a Stop condition, as shown in *Figure 9*.

5.9 Page write

The Page write mode allows up to four bytes to be written in a single write cycle, provided that they are all located in the same "row" in the memory: that is, the most significant memory address bits (b12-b2) are the same. If more bytes are sent than fit up to the end of the row, a condition known as "roll-over" occurs. This should be avoided, as data starts to become overwritten in an implementation-dependent way.

The bus master sends from one to four bytes of data, each of which is acknowledged by the device if the I2C_Write_Lock bit = 0 or the I2C_Password was correctly presented. If the I2C_Write_Lock_bit = 1 and the I2C_password are not presented, the contents of the addressed memory location are not modified, and each data byte is followed by a NoAck. After each byte is transferred, the internal byte address counter (inside the page) is incremented. The transfer is terminated by the bus master generating a Stop condition.

Figure 9. Write mode sequences with I2C_Write_Lock bit = 0 (data write enabled)

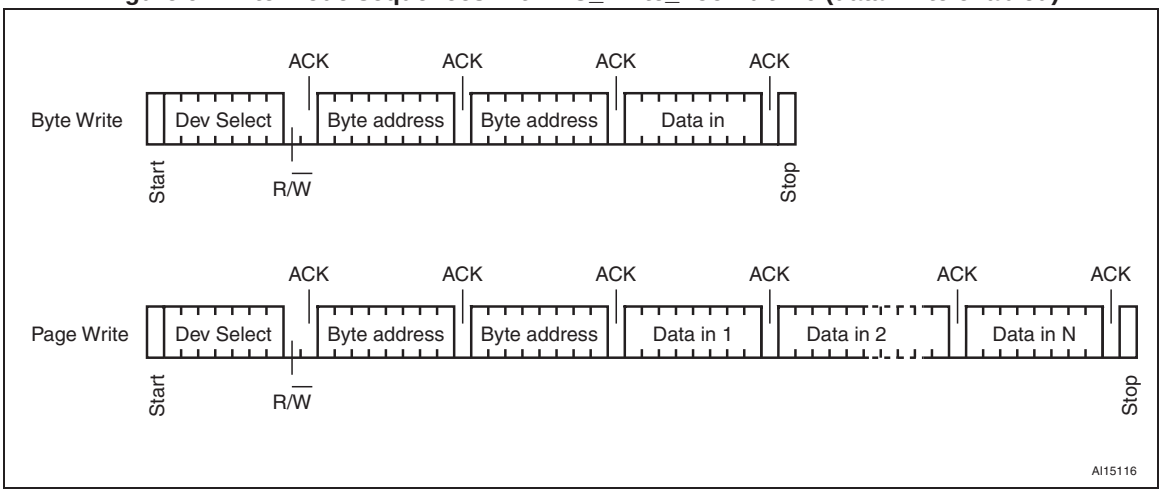
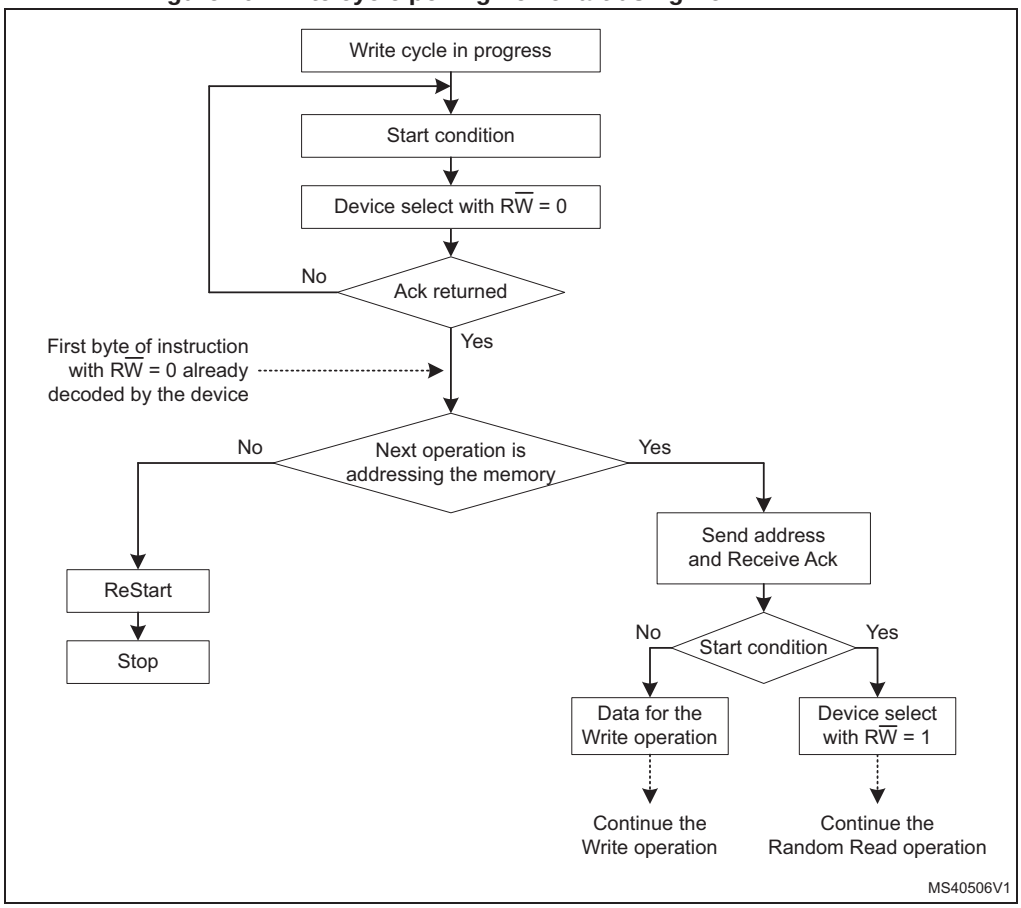


Figure 10. Write cycle polling flowchart using Ack



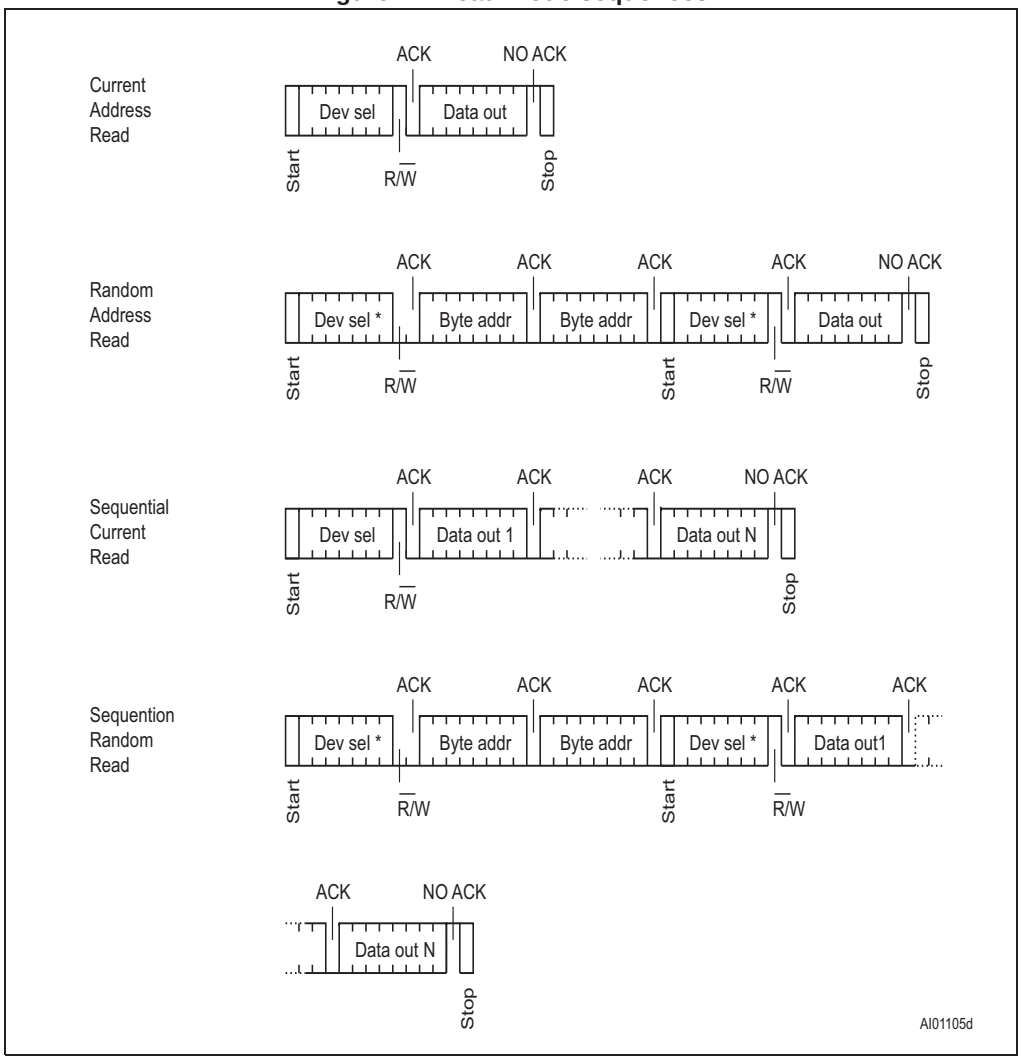
5.10 Minimizing system delays by polling on Ack

During the internal write cycle, the device disconnects itself from the bus, and writes a copy of the data from its internal latches to the memory cells. The maximum I²C write time (t_w) is shown in *Table 123*, but the typical time is shorter. To make use of this, a polling sequence can be used by the bus master.

The sequence, as shown in *Figure 10*, is:

1. Initial condition: a write cycle is in progress.
2. Step 1: the bus master issues a Start condition followed by a device select code (the first byte of the new instruction).
3. Step 2: if the device is busy with the internal write cycle, no Ack is returned and the bus master goes back to Step 1. If the device has terminated the internal write cycle, it responds with an Ack, indicating that the device is ready to receive the second part of the instruction (the first byte of this instruction having been sent during Step 1).

Figure 11. Read mode sequences



1. The seven most significant bits of the device select code of a random read (in the first and fourth bytes) must be identical.

5.11 Read operations

Read operations are performed independently of the state of the I2C_Write_Lock bit.

After the successful completion of a read operation, the device's internal address counter is incremented by one, to point to the next byte address.

5.12 Random Address Read

A dummy write is first performed to load the address into this address counter (as shown in *Figure 11*) but *without* sending a Stop condition. Then, the bus master sends another Start condition, and repeats the device select code, with the Read/Write bit (RW) set to 1. The device acknowledges this, and outputs the contents of the addressed byte. The bus master must *not* acknowledge the byte, and terminates the transfer with a Stop condition.

5.13 Current Address Read

For the Current Address Read operation, following a Start condition, the bus master only sends a device select code with the Read/Write bit (RW) set to 1. The device acknowledges this, and outputs the byte addressed by the internal address counter. The counter is then incremented. The bus master terminates the transfer with a Stop condition, as shown in *Figure 11*, *without* acknowledging the byte.

5.14 Sequential Read

This operation can be used after a Current Address Read or a Random Address Read. The bus master *does* acknowledge the data byte output, and sends additional clock pulses so that the device continues to output the next byte in sequence. To terminate the stream of bytes, the bus master must *not* acknowledge the last byte, and *must* generate a Stop condition, as shown in *Figure 11*.

The output data comes from consecutive addresses, with the internal address counter automatically incremented after each byte output. After the last memory address, the address counter "rolls over", and the device continues to output data from memory address 00h.

5.15 Acknowledge in Read mode

For all Read commands, the device waits, after each byte read, for an acknowledgment during the ninth bit time. If the bus master does not drive Serial Data (SDA) low during this time, the device terminates the data transfer and switches to its Standby mode.

5.16 M24LR64E-R I²C password security

The M24LR64E-R controls I²C sector write access using the 32-bit-long I²C password and the 64-bit I2C_Write_Lock bit area. The I²C password value is managed using two I²C commands: I²C present password and I²C write password.

5.16.1 I²C present password command description

The I²C present password command is used in I²C mode to present the password to the M24LR64E-R in order to modify the write access rights of all the memory sectors protected by the I2C_Write_Lock bits, including the password itself. If the presented password is correct, the access rights remain activated until the M24LR64E-R is powered off or until a new I²C present password command is issued.

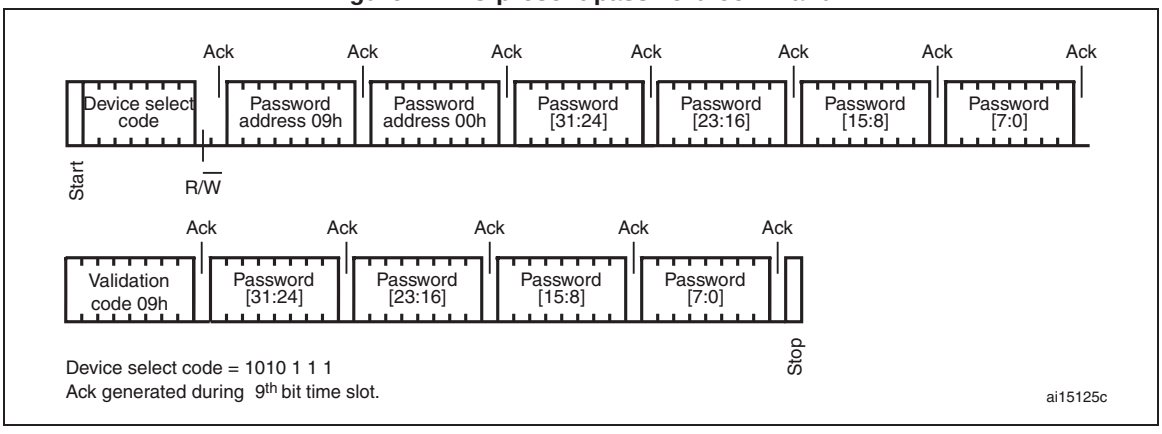
Following a Start condition, the bus master sends a device select code with the Read/$\overline{\text{Write}}$ bit (R$\overline{\text{W}}$) reset to 0 and the Chip Enable bit E2 at 1. The device acknowledges this, as shown in *Figure 12*, and waits for two I²C password address bytes, 09h and 00h. The device responds to each address byte with an acknowledge bit, and then waits for the four password data bytes, the validation code, 09h, and a resend of the four password data bytes. The most significant byte of the password is sent first, followed by the least significant bytes.

It is necessary to send the 32-bit password twice to prevent any data corruption during the sequence. If the two 32-bit passwords sent are not exactly the same, the M24LR64E-R does not start the internal comparison.

When the bus master generates a Stop condition immediately after the Ack bit (during the tenth bit time slot), an internal delay equivalent to the write cycle time is triggered. A Stop condition at any other time does not trigger the internal delay. During that delay, the M24LR64E-R compares the 32 received data bits with the 32 bits of the stored I²C password. If the values match, the write access rights to all protected sectors are modified after the internal delay. If the values do not match, the protected sectors remain protected.

During the internal delay, the serial data (SDA) signal is disabled internally, and the device does not respond to any requests.

Figure 12. I²C present password command



5.16.2 I²C write password command description

The I²C write password command is used to write a 32-bit block into the M24LR64E-R I²C password system area. This command is used in I²C mode to update the I²C password value. It cannot be used to update any of the RF passwords. After the write cycle, the new I²C password value is automatically activated. The I²C password value can only be modified after issuing a valid I²C present password command.

On delivery, the I²C default password value is set to 0000 0000h and is activated.

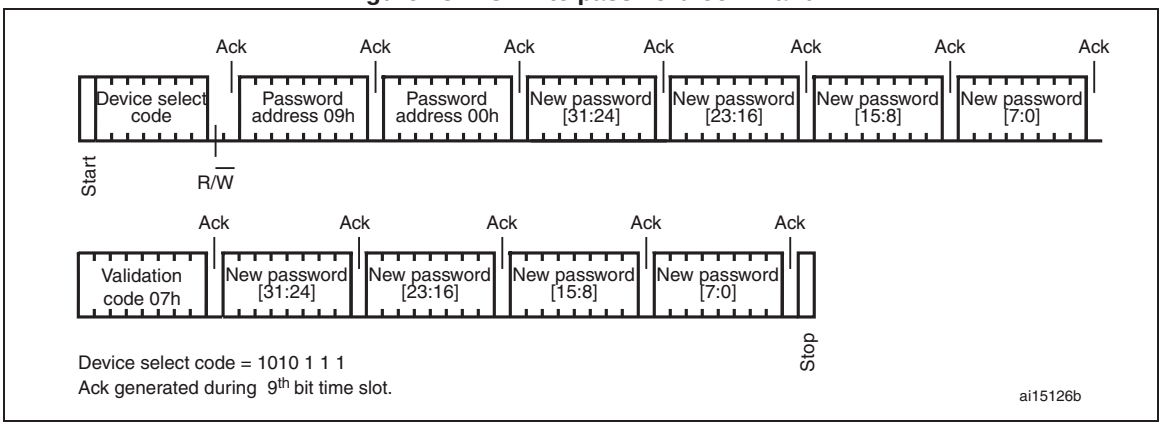
Following a Start condition, the bus master sends a device select code with the Read/$\overline{\text{Write}}$ bit ($\overline{\text{RW}}$) reset to 0 and the Chip Enable bit E2 at 1. The device acknowledges this, as shown in *Figure 13*, and waits for the two I²C password address bytes, 09h and 00h. The device responds to each address byte with an acknowledge bit, and then waits for the four password data bytes, the validation code, 07h, and a resend of the four password data bytes. The most significant byte of the password is sent first, followed by the least significant bytes.

It is necessary to send twice the 32-bit password to prevent any data corruption during the write sequence. If the two 32-bit passwords sent are not exactly the same, the M24LR64E-R does not modify the I²C password value.

When the bus master generates a Stop condition immediately after the Ack bit (during the tenth bit time slot), the internal write cycle is triggered. A Stop condition at any other time does not trigger the internal write cycle.

During the internal write cycle, the serial data (SDA) signal is disabled internally, and the device does not respond to any requests.

Figure 13. I²C write password command



6 M24LR64E-R memory initial state

The device is delivered with all bits in the user memory array set to 1 (each byte contains FFh).

The DSFID is programmed to FFh and the AFI is programmed to 00h.

Configuration byte set to F4h:

- Bit 7 to bit 4: all set to 1
- Bit 3: set to 0 (RF BUSY mode on RF WIP/BUSY pin)
- Bit 2: set to 1 (Energy harvesting not activated by default)
- Bit 1 and bit 0: set to 0

7 RF device operation

The M24LR64E-R is divided into 64 sectors of 32 blocks of 32 bits, as shown in *Table 5*. Each sector can be individually read- and/or write-protected using a specific lock or password command.

Read and Write operations are possible if the addressed block is not protected. During a Write, the 32 bits of the block are replaced by the new 32-bit value.

The M24LR64E-R also has a 64-bit block that is used to store the 64-bit unique identifier (UID). The UID is compliant with the ISO 15963 description, and its value is used during the anticollision sequence (Inventory). This block is not accessible by the user in RF device operation and its value is written by ST on the production line.

The M24LR64E-R also includes an AFI register in which the application family identifier is stored, and a DSFID register in which the data storage family identifier used in the anticollision algorithm is stored.

The M24LR64E-R has three 32-bit blocks in which the password codes are stored and an 8-bit Configuration byte in which the Energy harvesting mode and RF WIP/BUSY pin configuration is stored.

7.1 RF communication and energy harvesting

As the current consumption can affect the AC signal delivered by the antenna, RF communications with M24LR64E-R are not guaranteed during voltage delivery on the energy harvesting analog output V_{out}.

RF communication can disturb and possibly stop Energy Harvesting mode.

7.2 Commands

The M24LR64E-R supports the following commands:

- ***Inventory***, used to perform the anticollision sequence.
- ***Stay quiet***, used to put the M24LR64E-R in quiet mode, where it does not respond to any inventory command.
- ***Select***, used to select the M24LR64E-R. After this command, the M24LR64E-R processes all Read/Write commands with Select_flag set.
- ***Reset to ready***, used to put the M24LR64E-R in the ready state.
- ***Read block***, used to output the 32 bits of the selected block and its locking status.
- ***Write block***, used to write the 32-bit value in the selected block, provided that it is not locked.
- ***Read multiple blocks***, used to read the selected blocks and send back their value.
- ***Write AFI***, used to write the 8-bit value in the AFI register.
- ***Lock AFI***, used to lock the AFI register.
- ***Write DSFID***, used to write the 8-bit value in the DSFID register.
- ***Lock DSFID***, used to lock the DSFID register.
- ***Get system info***, used to provide the system information value.
- ***Get multiple block security status***, used to send the security status of the selected block.
- ***Initiate***, used to trigger the tag response to the Inventory initiated sequence.
- ***Inventory initiated***, used to perform the anticollision sequence triggered by the Initiate command.
- ***Write-sector password***, used to write the 32 bits of the selected password.
- **Lock-sector**, used to write the sector security status bits of the selected sector.
- ***Present-sector password***, enables the user to present a password to unprotect the user blocks linked to this password.
- ***Fast initiate***, used to trigger the tag response to the Inventory initiated sequence.
- ***Fast inventory initiated***, used to perform the anticollision sequence triggered by the Initiate command.
- ***Fast read single block***, used to output the 32 bits of the selected block and its locking status.
- ***Fast read multiple blocks***, used to read the selected blocks and send back their value.
- ***ReadCfg,*** used to read the 8-bit Configuration byte and send back its value.
- ***WriteEHCfg***, used to write the energy harvesting configuration bits into the Configuration byte.
- ***WriteDOCfg***, used to write the RF WIP/BUSY pin configuration bit into the Configuration byte.
- ***SetRstEHEn***, used to set or reset the EH_enable bit into the volatile Control register.
- ***CheckEHEn***, used to send back the value of the volatile Control register.

7.3 Initial dialog for vicinity cards

The dialog between the vicinity coupling device or VCD (commonly the “RF reader”) and the vicinity integrated circuit card or VICC (M24LR64E-R) takes place as follows:

- activation of the M24LR64E-R by the RF operating field of the VCD
- transmission of a command by the VCD
- transmission of a response by the M24LR64E-R.

These operations use the RF power transfer and communication signal interface described below (see *Power transfer*, *Frequency* and *Operating field*). This technique is called RTF (Reader talks first).

7.3.1 Power transfer

Power is transferred to the M24LR64E-R by radio frequency at 13.56 MHz via coupling antennas in the M24LR64E-R and the VCD. The RF operating field of the VCD is transformed on the M24LR64E-R antenna to an AC voltage which is rectified, filtered and internally regulated.

During communications, the amplitude modulation (ASK) on this received signal is demodulated by the ASK demodulator.

7.3.2 Frequency

The ISO 15693 standard defines the carrier frequency (f_C) of the operating field as 13.56 MHz ±7 kHz.

7.3.3 Operating field

The M24LR64E-R operates continuously between the minimum and maximum values of the electromagnetic field H defined in *Table 125*. The VCD has to generate a field within these limits.

8 Communication signal from VCD to M24LR64E-R

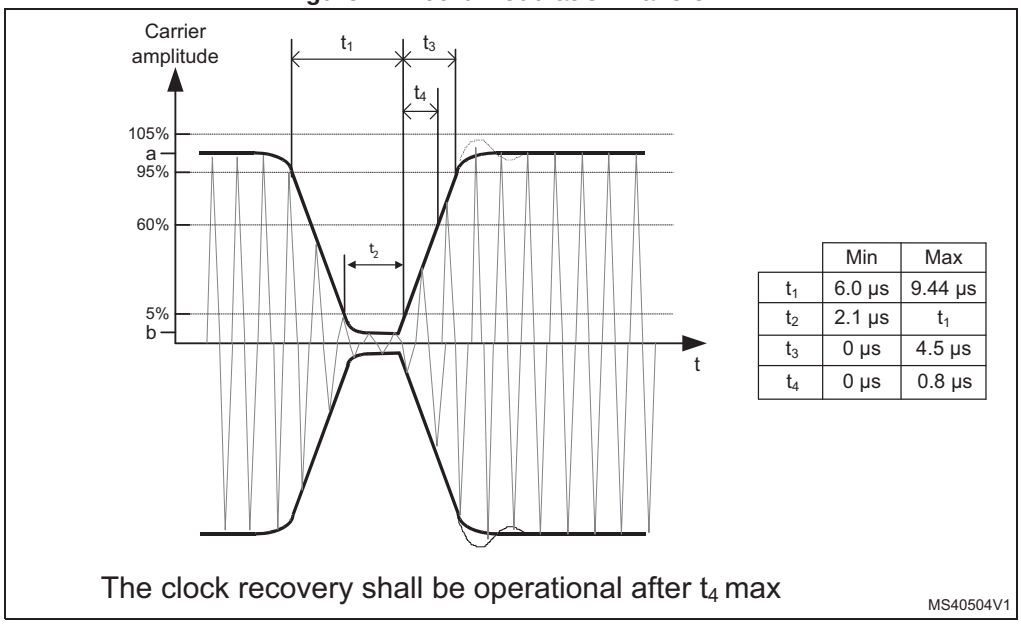
Communications between the VCD and the M24LR64E-R take place using the modulation principle of ASK (Amplitude shift keying). Two modulation indexes are used, 10% and 100%. The M24LR64E-R decodes both. The VCD determines which index is used.

The modulation index is defined as [a – b]/[a + b], where a is the peak signal amplitude, and b the minimum signal amplitude of the carrier frequency.

Depending on the choice made by the VCD, a “pause” is created as described in *Figure 14* and *Figure 15*.

The M24LR64E-R is operational for the 100% modulation index or for any degree of modulation index between 10% and 30% (see *Table 125*).

Figure 14. 100% modulation waveform

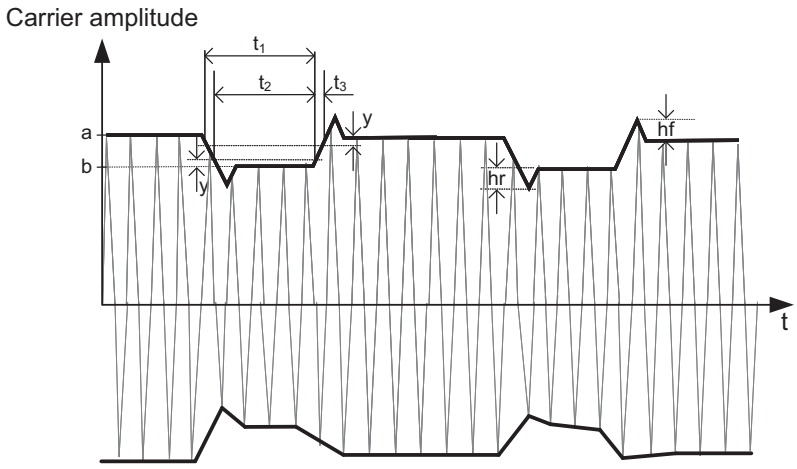


	Min	Max
t_1	6.0 µs	9.44 µs
t_2	2.1 µs	t_1
t_3	0 µs	4.5 µs
t_4	0 µs	0.8 µs

Table 19. 10% modulation parameters

Symbol	Parameter definition	Value
hr	0.1 x (a – b)	max
hf	0.1 x (a – b)	max

Figure 15. 10% modulation waveform



	Min	Max
t_1	6.0 µs	9.44 µs
t_2	3.0 µs	t_1
t_3	0	4.5 µs
Modulation index	10%	30%

y	0.05 (a-b)
hf, hr	0.1 (a-b) max

The VICC shall be operational for any value of modulation index between 10 and 30%.

MS40501V1

9 Data rate and data coding

The data coding implemented in the M24LR64E-R uses pulse position modulation. Both data coding modes that are described in the ISO15693 are supported by the M24LR64E-R. The selection is made by the VCD and indicated to the M24LR64E-R within the start of frame (SOF).

9.1 Data coding mode: 1 out of 256

The value of a single byte is represented by the position of one pause. The position of the pause on one of 256 successive time periods of 18.88 µs (256/f_C) determines the value of the byte. In this case, the transmission of one byte takes 4.833 ms and the resulting data rate is 1.65 Kbits/s (f_C/8192).

Figure 16 illustrates this pulse position modulation technique. In this figure, data E1h (225 decimal) is sent by the VCD to the M24LR64E-R.

The pause occurs during the second half of the position of the time period that determines the value, as shown in *Figure 17*.

A pause during the first period transmits the data value 00h. A pause during the last period transmits the data value FFh (255 decimal).

Figure 16. 1 out of 256 coding mode

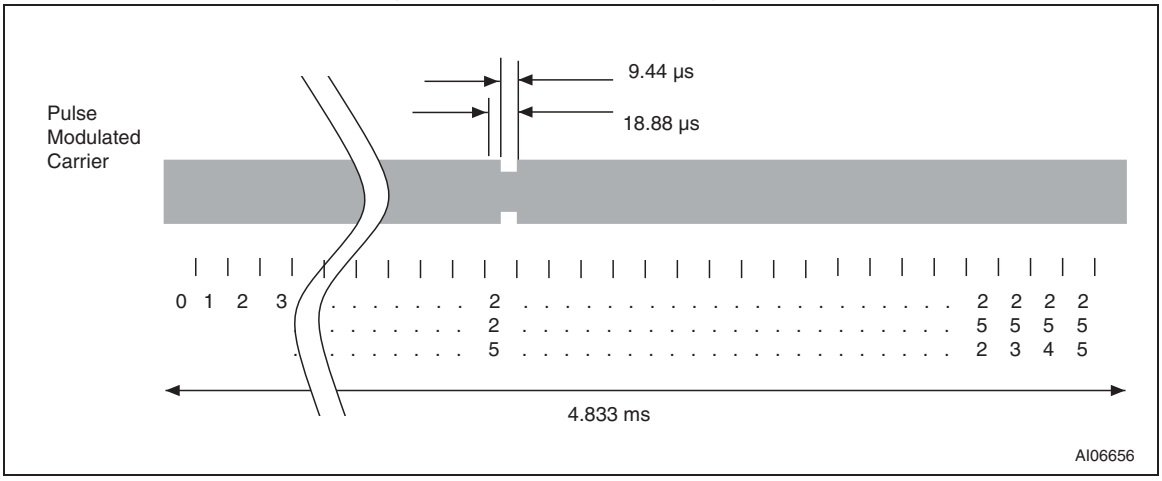
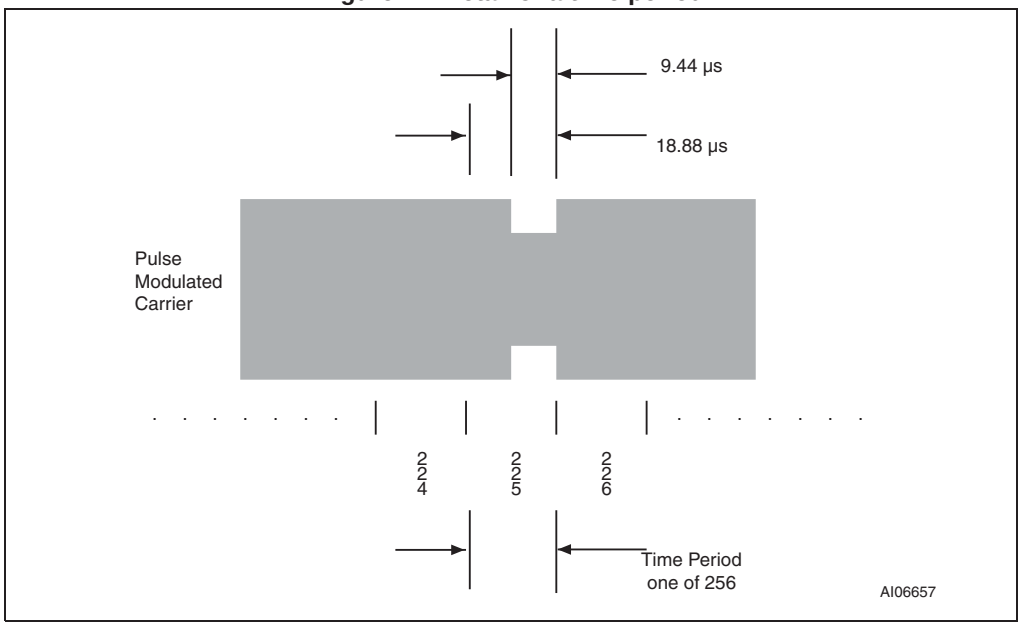


Figure 17. Detail of a time period



9.2 Data coding mode: 1 out of 4

The value of two bits is represented by the position of one pause. The position of the pause on one of four successive time periods of 18.88 µs ($256/f_C$) determines the value of the two bits. Four successive pairs of bits form a byte, where the least significant pair of bits is transmitted first.

In this case, the transmission of one byte takes 302.08 µs and the resulting data rate is 26.48 Kbits/s ($f_C/512$). *Figure 18* illustrates the 1 out of 4 pulse position technique and coding. *Figure 19* shows the transmission of E1h (225d - 1110 0001b) by the VCD.

Figure 18. 1 out of 4 coding mode

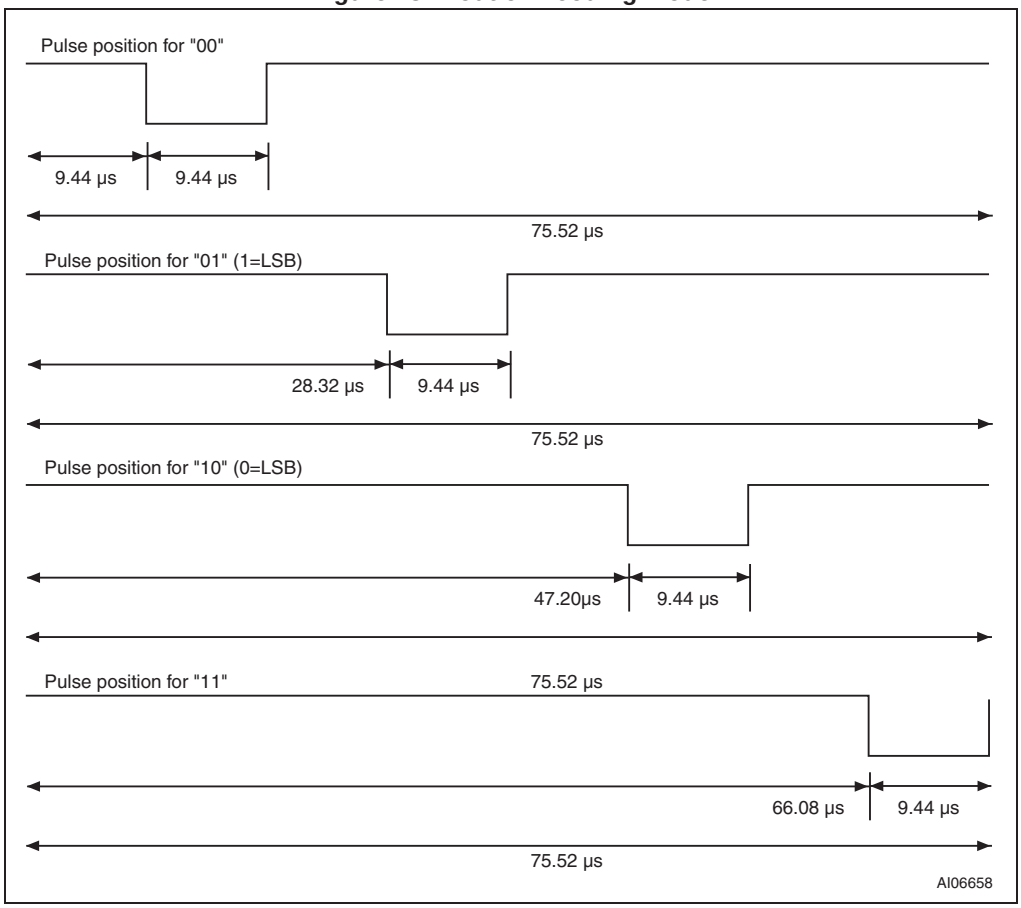
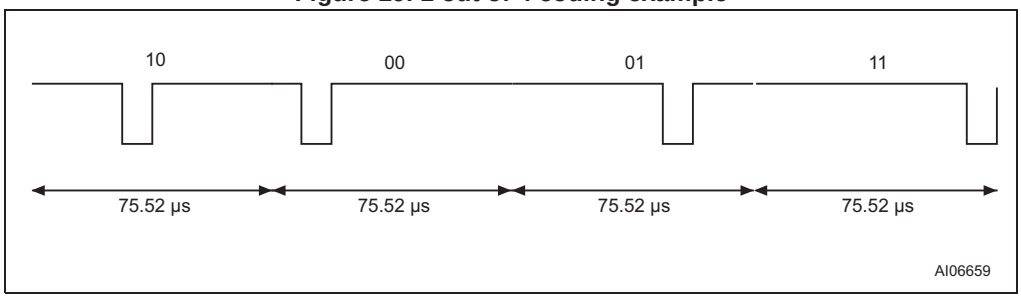


Figure 19. 1 out of 4 coding example



9.3 VCD to M24LR64E-R frames

Frames are delimited by a start of frame (SOF) and an end of frame (EOF). They are implemented using code violation. Unused options are reserved for future use.

The M24LR64E-R is ready to receive a new command frame from the VCD 311.5 µs after sending a response frame to the VCD.

The M24LR64E-R takes a power-up time of 0.1 ms after being activated by the powering field. After this delay, the M24LR64E-R is ready to receive a command frame from the VCD.

9.4 Start of frame (SOF)

The SOF defines the data coding mode the VCD is to use for the following command frame. The SOF sequence described in *Figure 20* selects the 1 out of 256 data coding mode. The SOF sequence described in *Figure 21* selects the 1 out of 4 data coding mode. The EOF sequence for either coding mode is described in *Figure 22*.

Figure 20. SOF to select 1 out of 256 data coding mode

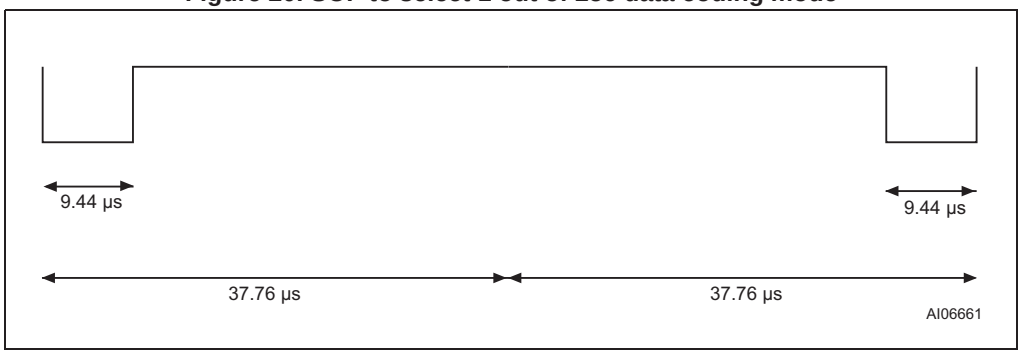


Figure 21. SOF to select 1 out of 4 data coding mode

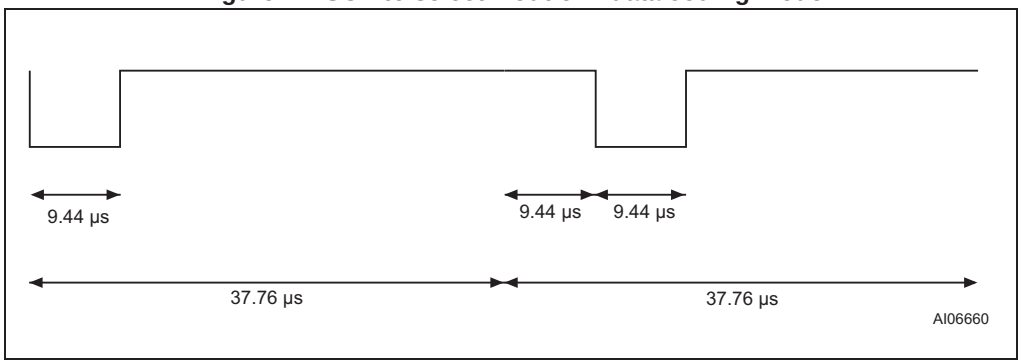
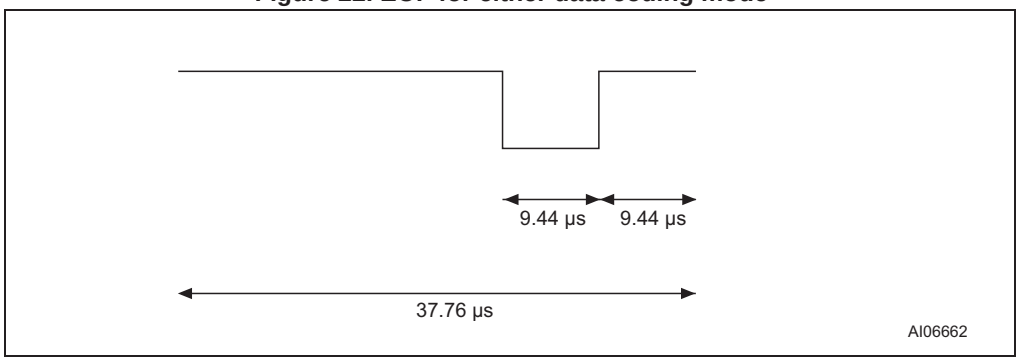


Figure 22. EOF for either data coding mode



10 Communication signal from M24LR64E-R to VCD

The M24LR64E-R has several modes defined for some parameters, so that it can operate in various noise environments and meet various application requirements.

10.1 Load modulation

The M24LR64E-R is capable of communicating to the VCD via an inductive coupling area whereby the carrier is loaded to generate a subcarrier with frequency f_S. The subcarrier is generated by switching a load in the M24LR64E-R.

The load-modulated amplitude received on the VCD antenna must be of at least 10 mV when measured, as described in the test methods defined in International Standard ISO10373-7.

10.2 Subcarrier

The M24LR64E-R supports the one-subcarrier and two-subcarriers response formats. These formats are selected by the VCD using the first bit in the protocol header. When one subcarrier is used, the frequency f_{S1} of the subcarrier load modulation is 423.75 kHz (f_C/32). When two subcarriers are used, the frequency f_{S1} is 423.75 kHz (f_C/32), and frequency f_{S2} is 484.28 kHz (f_C/28). When using the two-subcarriers mode, the M24LR64E-R generates a continuous phase relationship between f_{S1} and f_{S2}.

10.3 Data rates

The M24LR64E-R can respond using the low or the high data rate format. The selection of the data rate is made by the VCD using the second bit in the protocol header. For fast commands, the selected data rate is multiplied by two. *Table 20* shows the different data rates produced by the M24LR64E-R using the different response format combinations.

Table 20. Response data rates

Data rate		One subcarrier	Two subcarriers
Low	Standard commands	6.62 Kbit/s (f_c/2048)	6.67 Kbit/s (f_c/2032)
	Fast commands	13.24 Kbit/s (f_c/1024)	Not applicable
High	Standard commands	26.48 Kbit/s (f_c/512)	26.69 Kbit/s (f_c/508)
	Fast commands	52.97 Kbit/s (f_c/256)	Not applicable

11 Bit representation and coding

Data bits are encoded using Manchester coding, according to the following schemes. For the low data rate, same subcarrier frequency or frequencies is/are used. In this case, the number of pulses is multiplied by 4 and all times increase by this factor. For the Fast commands using one subcarrier, all pulse numbers and times are divided by 2.

11.1 Bit coding using one subcarrier

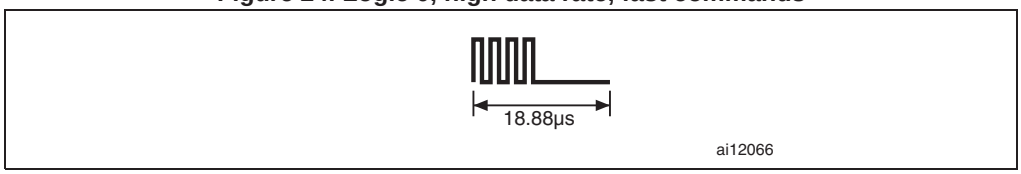
11.1.1 High data rate

A logic 0 starts with eight pulses at 423.75 kHz ($f_C/32$) followed by an unmodulated time of 18.88 µs, as shown in *Figure 23*.

Figure 23. Logic 0, high data rate

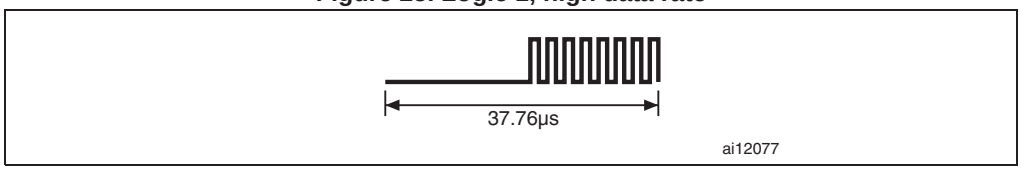
For the fast commands, a logic 0 starts with four pulses at 423.75 kHz ($f_C/32$) followed by an unmodulated time of 9.44 µs, as shown in *Figure 24*.

Figure 24. Logic 0, high data rate, fast commands



A logic 1 starts with an unmodulated time of 18.88 µs followed by eight pulses at 423.75 kHz ($f_C/32$), as shown in *Figure 25*.

Figure 25. Logic 1, high data rate



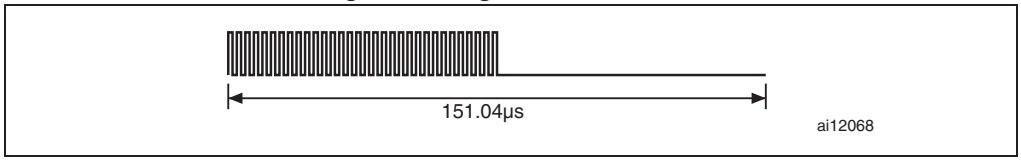
For the Fast commands, a logic 1 starts with an unmodulated time of 9.44 µs followed by four pulses of 423.75 kHz ($f_C/32$), as shown in *Figure 26*.

Figure 26. Logic 1, high data rate, fast commands

11.1.2 Low data rate

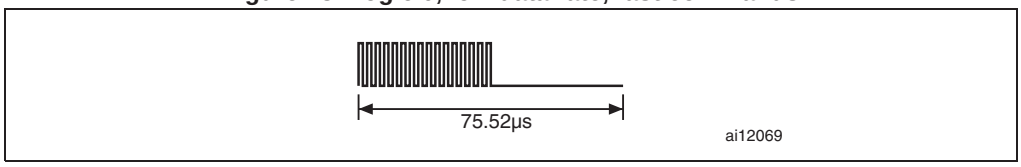
A logic 0 starts with 32 pulses at 423.75 kHz (f_C/32) followed by an unmodulated time of 75.52 µs, as shown in *Figure 27*.

Figure 27. Logic 0, low data rate



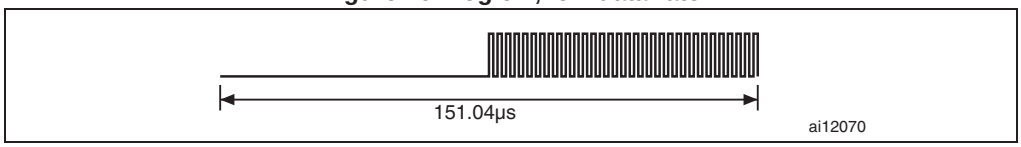
For the Fast commands, a logic 0 starts with 16 pulses at 423.75 kHz (f_C/32) followed by an unmodulated time of 37.76 µs, as shown in *Figure 28*.

Figure 28. Logic 0, low data rate, fast commands



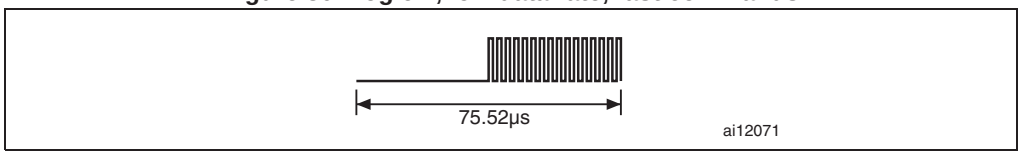
A logic 1 starts with an unmodulated time of 75.52 µs followed by 32 pulses at 423.75 kHz (f_C/32), as shown in *Figure 29*.

Figure 29. Logic 1, low data rate



For the Fast commands, a logic 1 starts with an unmodulated time of 37.76 µs followed by 16 pulses at 423.75 kHz (f_C/32), as shown in *Figure 30*.

Figure 30. Logic 1, low data rate, fast commands

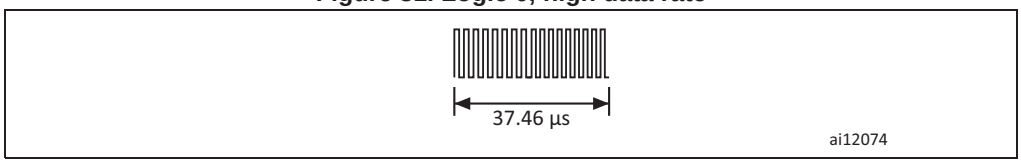


11.2 Bit coding using two subcarriers

11.2.1 High data rate

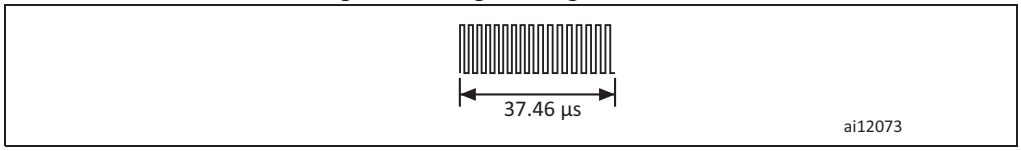
A logic 0 starts with eight pulses at 423.75 kHz ($f_C/32$) followed by nine pulses at 484.28 kHz ($f_C/28$), as shown in *Figure 31*. Bit coding using two subcarriers is not supported for the Fast commands.

Figure 31. Logic 0, high data rate



A logic 1 starts with nine pulses at 484.28 kHz ($f_C/28$) followed by eight pulses at 423.75 kHz ($f_C/32$), as shown in *Figure 32*. Bit coding using two subcarriers is not supported for the Fast commands.

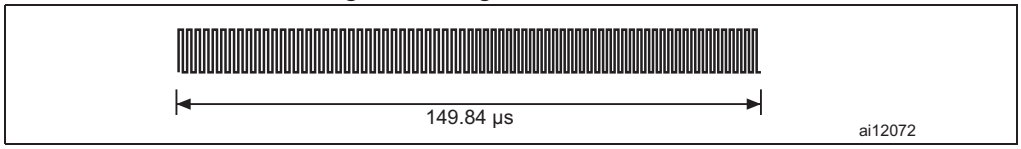
Figure 32. Logic 1, high data rate



11.2.2 Low data rate

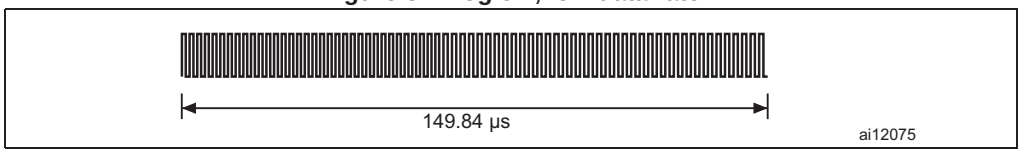
A logic 0 starts with 32 pulses at 423.75 kHz ($f_C/32$) followed by 36 pulses at 484.28 kHz ($f_C/28$), as shown in *Figure 33*. Bit coding using two subcarriers is not supported for the Fast commands.

Figure 33. Logic 0, low data rate



A logic 1 starts with 36 pulses at 484.28 kHz ($f_C/28$) followed by 32 pulses at 423.75 kHz ($f_C/32$) as shown in *Figure 34*. Bit coding using two subcarriers is not supported for the Fast commands.

Figure 34. Logic 1, low data rate



12 M24LR64E-R to VCD frames

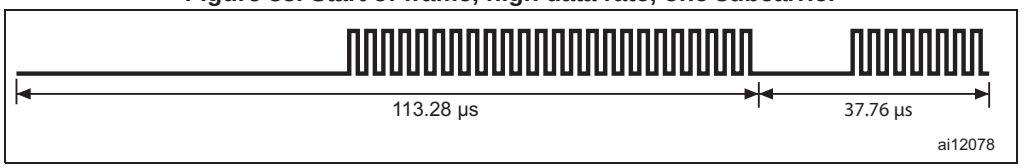
Frames are delimited by an SOF and an EOF. They are implemented using code violation. Unused options are reserved for future use. For the low data rate, the same subcarrier frequency or frequencies is/are used. In this case, the number of pulses is multiplied by 4. For the Fast commands using one subcarrier, all pulse numbers and times are divided by 2.

12.1 SOF when using one subcarrier

12.1.1 High data rate

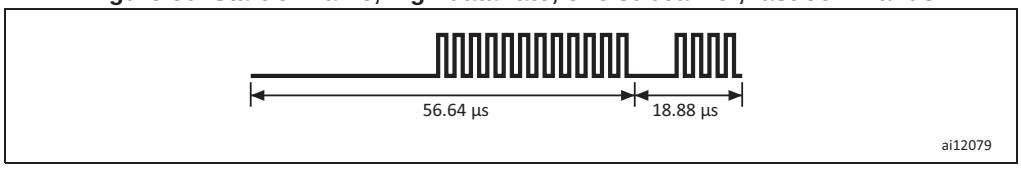
The SOF includes an unmodulated time of 56.64 µs, followed by 24 pulses at 423.75 kHz ($f_C/32$), and a logic 1 that consists of an unmodulated time of 18.88 µs followed by eight pulses at 423.75 kHz, as shown in *Figure 35*.

Figure 35. Start of frame, high data rate, one subcarrier



For the Fast commands, the SOF comprises an unmodulated time of 28.32 µs, followed by 12 pulses at 423.75 kHz ($f_C/32$), and a logic 1 that consists of an unmodulated time of 9.44 µs followed by four pulses at 423.75 kHz, as shown in *Figure 36*.

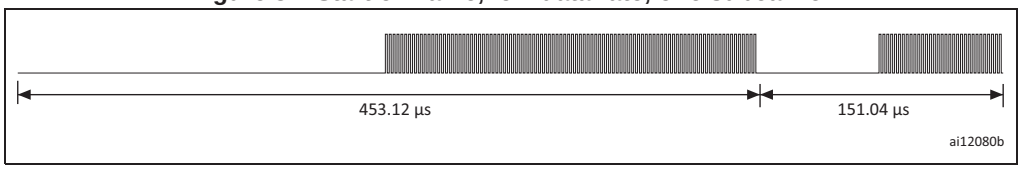
Figure 36. Start of frame, high data rate, one subcarrier, fast commands



12.1.2 Low data rate

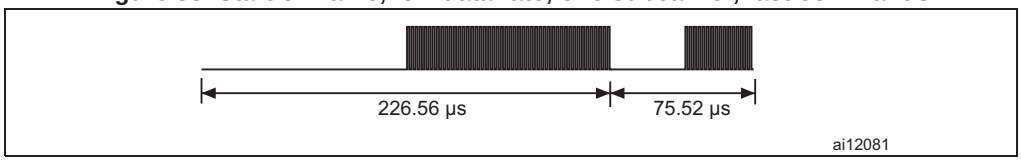
The SOF comprises an unmodulated time of 226.56 µs, followed by 96 pulses at 423.75 kHz ($f_C/32$), and a logic 1 that consists of an unmodulated time of 75.52 µs followed by 32 pulses at 423.75 kHz, as shown in *Figure 37*.

Figure 37. Start of frame, low data rate, one subcarrier



For the Fast commands, the SOF comprises an unmodulated time of 113.28 µs, followed by 48 pulses at 423.75 kHz (f_C/32), and a logic 1 that includes an unmodulated time of 37.76 µs followed by 16 pulses at 423.75 kHz, as shown in *Figure 38*.

Figure 38. Start of frame, low data rate, one subcarrier, fast commands



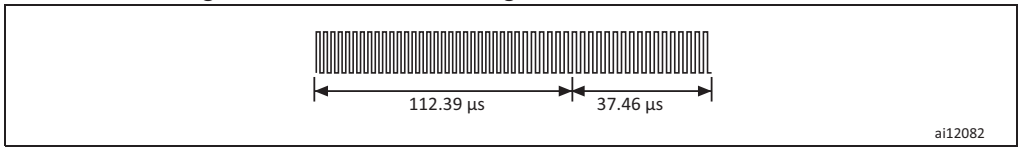
12.2 SOF when using two subcarriers

12.2.1 High data rate

The SOF comprises 27 pulses at 484.28 kHz (f_C/28), followed by 24 pulses at 423.75 kHz (f_C/32), and a logic 1 that includes nine pulses at 484.28 kHz followed by eight pulses at 423.75 kHz, as shown in *Figure 39*.

Bit coding using two subcarriers is not supported for the Fast commands.

Figure 39. Start of frame, high data rate, two subcarriers

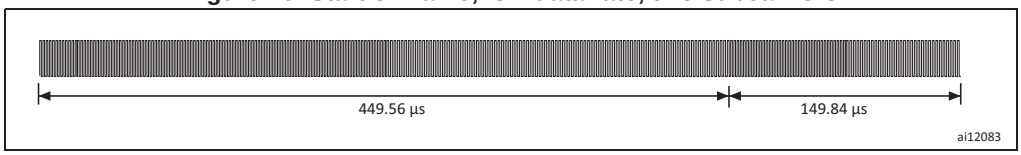


12.2.2 Low data rate

The SOF comprises 108 pulses at 484.28 kHz (f_C/28), followed by 96 pulses at 423.75 kHz (f_C/32), and a logic 1 that includes 36 pulses at 484.28 kHz followed by 32 pulses at 423.75 kHz, as shown in *Figure 40*.

Bit coding using two subcarriers is not supported for the Fast commands.

Figure 40. Start of frame, low data rate, two subcarriers

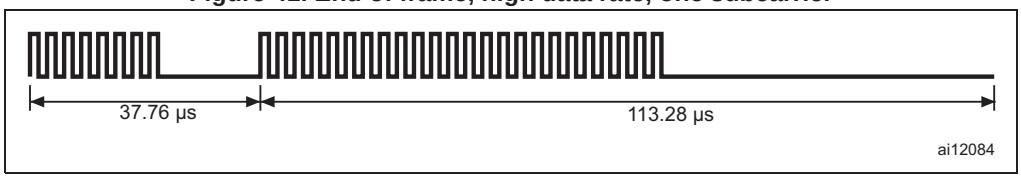


12.3 EOF when using one subcarrier

12.3.1 High data rate

The EOF comprises a logic 0 that includes eight pulses at 423.75 kHz and an unmodulated time of 18.88 µs, followed by 24 pulses at 423.75 kHz (f_C/32), and by an unmodulated time of 56.64 µs, as shown in *Figure 41*.

Figure 41. End of frame, high data rate, one subcarrier



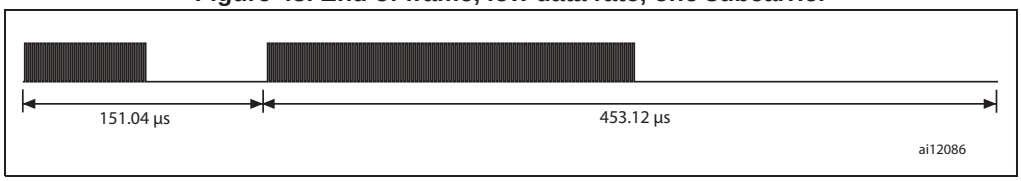
For the Fast commands, the EOF comprises a logic 0 that includes four pulses at 423.75 kHz and an unmodulated time of 9.44 µs, followed by 12 pulses at 423.75 kHz (f_C/32) and an unmodulated time of 37.76 µs, as shown in *Figure 42*.

Figure 42. End of frame, high data rate, one subcarrier, fast commands

12.3.2 Low data rate

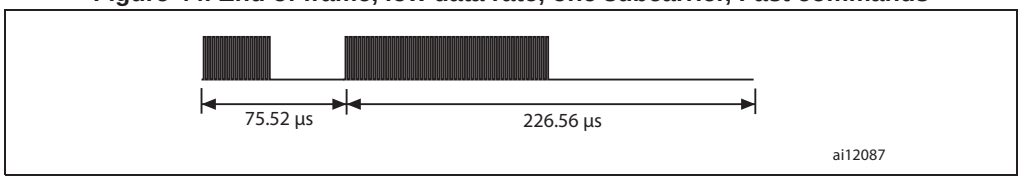
The EOF comprises a logic 0 that includes 32 pulses at 423.75 kHz and an unmodulated time of 75.52 µs, followed by 96 pulses at 423.75 kHz (f_C/32) and an unmodulated time of 226.56 µs, as shown in *Figure 43*.

Figure 43. End of frame, low data rate, one subcarrier



For the Fast commands, the EOF comprises a logic 0 that includes 16 pulses at 423.75 kHz and an unmodulated time of 37.76 µs, followed by 48 pulses at 423.75 kHz (f_C/32) and an unmodulated time of 113.28 µs, as shown in *Figure 44*.

Figure 44. End of frame, low data rate, one subcarrier, Fast commands



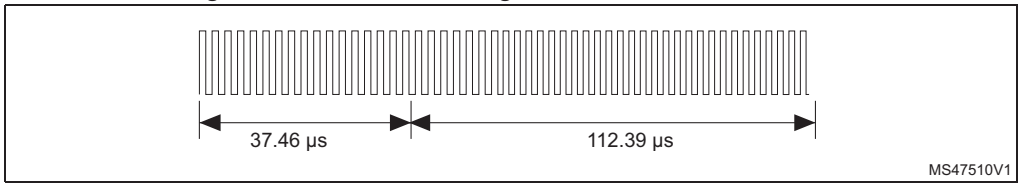
12.4 EOF when using two subcarriers

12.4.1 High data rate

The EOF comprises a logic 0 that includes eight pulses at 423.75 kHz and nine pulses at 484.28 kHz, followed by 24 pulses at 423.75 kHz (f_C/32) and 27 pulses at 484.28 kHz (f_C/28), as shown in *Figure 45*.

Bit coding using two subcarriers is not supported for the Fast commands.

Figure 45. End of frame, high data rate, two subcarriers

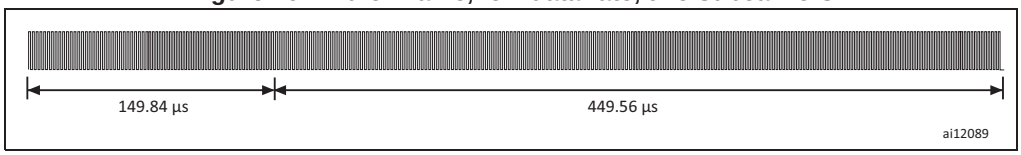


12.4.2 Low data rate

The EOF comprises a logic 0 that includes 32 pulses at 423.75 kHz and 36 pulses at 484.28 kHz, followed by 96 pulses at 423.75 kHz (f_C/32) and 108 pulses at 484.28 kHz (f_C/28), as shown in *Figure 46*.

Bit coding using two subcarriers is not supported for the Fast commands.

Figure 46. End of frame, low data rate, two subcarriers



13 Unique identifier (UID)

The M24LR64E-R is uniquely identified by a 64-bit unique identifier (UID). This UID complies with ISO/IEC 15963 and ISO/IEC 7816-6. The UID is a read-only code and comprises:

- eight MSBs with a value of E0h,
- the IC manufacturer code “ST 02h” on 8 bits (ISO/IEC 7816-6/AM1),
- a unique serial number on 48 bits.

Table 21. UID format

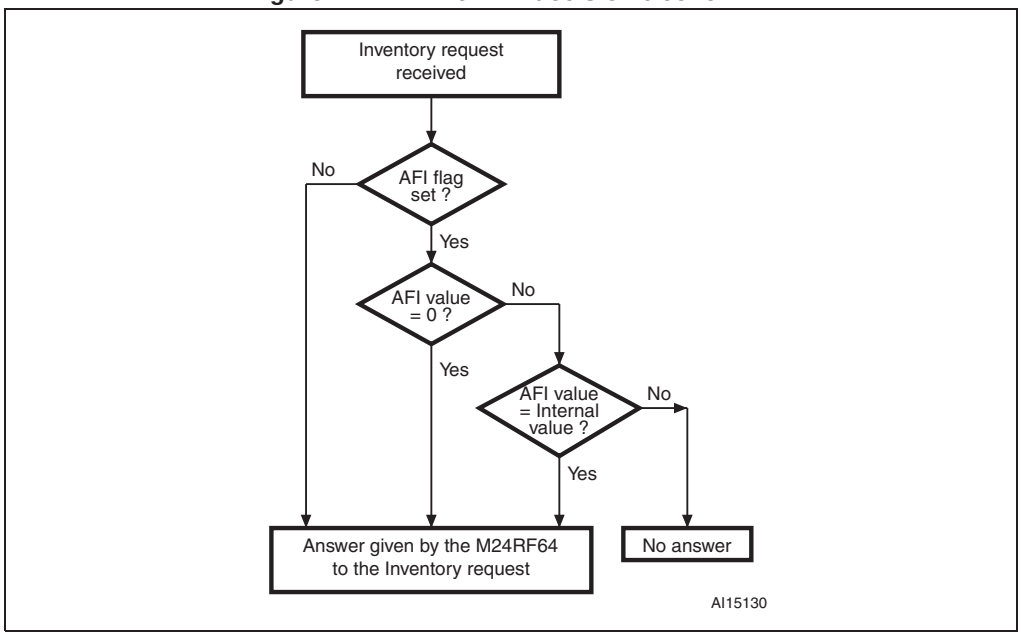
MSB					LSB
63	56	55	48	47	0
0xE0		0x02		Unique serial number	

With the UID, each M24LR64E-R can be addressed uniquely and individually during the anticollision loop and for one-to-one exchanges between a VCD and an M24LR64E-R.

14 Application family identifier (AFI)

The AFI (application family identifier) represents the type of application targeted by the VCD and is used to identify, among all the M24LR64E-Rs present, only those that meet the required application criteria.

Figure 47. M24LR64E-R decision tree for AFI



The AFI is programmed by the M24LR64E-R issuer (or purchaser) in the AFI register. Once programmed and locked, it can no longer be modified.

The most significant nibble of the AFI is used to code one specific or all application families.

The least significant nibble of the AFI is used to code one specific or all application subfamilies. Subfamily codes different from 0 are proprietary.

See also ISO 15693-3 documentation.

15 Data storage format identifier (DSFID)

The data storage format identifier indicates how the data is structured in the M24LR64E-R memory. The logical organization of data can be known instantly using the DSFID. It can be programmed and locked using the Write DSFID and Lock DSFID commands.

15.1 CRC

The CRC used in the M24LR64E-R is calculated as per the definition in ISO/IEC 13239. The initial register contents are all 1s: “FFFF”.

The two-byte CRC is appended to each request and response, within each frame, before the EOF. The CRC is calculated on all the bytes after the SOF up to the CRC field.

Upon reception of a request from the VCD, the M24LR64E-R verifies that the CRC value is valid. If it is invalid, the M24LR64E-R discards the frame and does not answer the VCD.

Upon reception of a response from the M24LR64E-R, it is recommended that the VCD verifies whether the CRC value is valid. If it is invalid, actions to be performed are left to the VCD designer judgment.

The CRC is transmitted least significant byte first. Each byte is transmitted least significant bit first.

Table 22. CRC transmission rules

LSByte		LSByte	
LSBit	**MSBit**	**LSBit**	**MSBit**
CRC 16 (8 bits)		CRC 16 (8 bits)	

16 M24LR64E-R protocol description

The transmission protocol (or simply “the protocol”) defines the mechanism used to exchange instructions and data between the VCD and the M24LR64E-R in both directions. It is based on the concept of “VCD talks first”.

This means that an M24LR64E-R does not start transmitting unless it has received and properly decoded an instruction sent by the VCD. The protocol is based on an exchange of:

- a request from the VCD to the M24LR64E-R,
- a response from the M24LR64E-R to the VCD.

Each request and each response are contained in a frame. The frame delimiters (SOF, EOF) are described in *Section 12*.

Each request consists of:

- a request SOF (see *Figure 20* and *Figure 21*),
- flags,
- a command code,
- parameters depending on the command,
- application data,
- a 2-byte CRC,
- a request EOF (see *Figure 22*).

Each response consists of:

- an answer SOF (see *Figure 35* to *Figure 40*),
- flags,
- parameters depending on the command,
- application data,
- a 2-byte CRC,
- an answer EOF (see *Figure 41* to *Figure 46*).

The protocol is bit-oriented. The number of bits transmitted in a frame is a multiple of eight (8), that is an integer number of bytes.

A single-byte field is transmitted least significant bit (LSBit) first. A multiple-byte field is transmitted least significant byte (LSByte) first and each byte is transmitted least significant bit (LSBit) first.

The setting of the flags indicates the presence of the optional fields. When the flag is set (to one), the field is present. When the flag is reset (to zero), the field is absent.

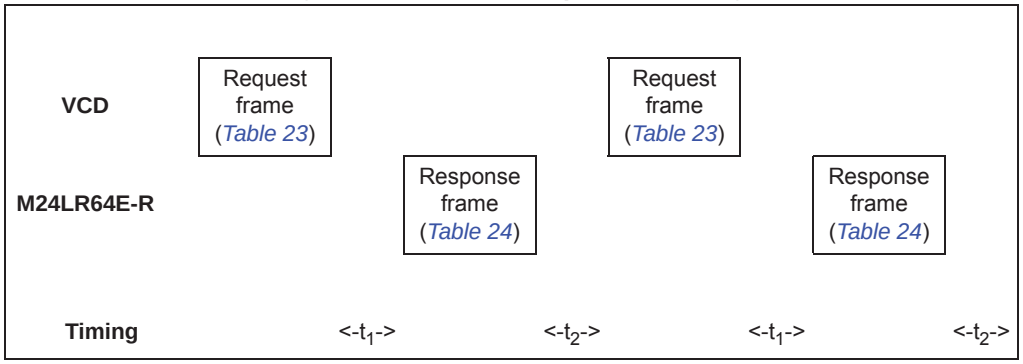
Table 23. VCD request frame format

Request SOF	Request_flags	Command code	Parameters	Data	2-byte CRC	Request EOF

Table 24. M24LR64E-R Response frame format

Response SOF	Response_flags	Parameters	Data	2-byte CRC	Response EOF

Figure 48. M24LR64E-R protocol timing



17 M24LR64E-R states

An M24LR64E-R can be in one of four states:

- Power-off
- Ready
- Quiet
- Selected

Transitions between these states are specified in *Figure 49* and *Table 25*.

17.1 Power-off state

The M24LR64E-R is in the Power-off state when it does not receive enough energy from the VCD.

17.2 Ready state

The M24LR64E-R is in the Ready state when it receives enough energy from the VCD. When in the Ready state, the M24LR64E-R answers any request where the Select_flag is not set.

17.3 Quiet state

When in the Quiet state, the M24LR64E-R answers any request except for Inventory requests with the Address_flag set.

17.4 Selected state

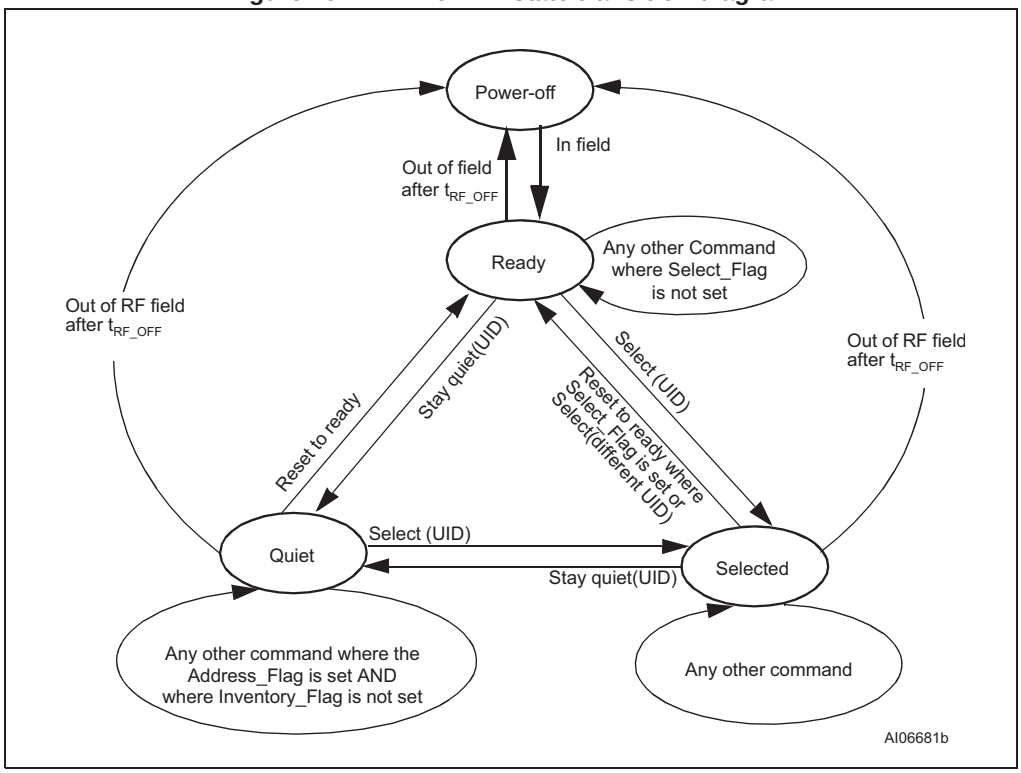
In the Selected state, the M24LR64E-R answers any request in all modes (see *Section 18*):

- Request in Select mode with the Select_flag set
- Request in Addressed mode if the UID matches
- Request in Non-Addressed mode as it is the mode for general requests

Table 25. M24LR64E-R response depending on Request_flags

Flags	Address_flag		Select_flag	
	1 Addressed	0 Non addressed	1 Selected	0 Non selected
M24LR64E-R in Ready or Selected state (Devices in Quiet state do not answer)	-	X	-	X
M24LR64E-R in Selected state	-	X	X	-
M24LR64E-R in Ready, Quiet or Selected state (the device which matches the UID)	X	-	-	X
Error (03h)	X	-	X	-

Figure 49. M24LR64E-R state transition diagram



1. The M24LR64E-R returns to the Power Off state if the tag is out of the RF field for at least t_{RF_OFF}. Refer to application note AN4125 for more information.
2. The intention of the state transition method is that only one M24LR64E-R should be in the Selected state at a time.

18 Modes

The term “mode” refers to the mechanism used in a request to specify the set of M24LR64E-Rs that answers the request.

18.1 Addressed mode

When the Address_flag is set to 1 (Addressed mode), the request contains the Unique ID (UID) of the addressed M24LR64E-R.

Any M24LR64E-R that receives a request with the Address_flag set to 1 compares the received Unique ID to its own. If it matches, then the M24LR64E-R executes the request (if possible) and returns a response to the VCD as specified in the command description.

If the UID does not match, then it remains silent.

18.2 Non-addressed mode (general request)

When the Address_flag is cleared to 0 (Non-Addressed mode), the request does not contain a Unique ID. Any M24LR64E-R receiving a request with the Address_flag cleared to 0 executes it and returns a response to the VCD as specified in the command description.

18.3 Select mode

When the Select_flag is set to 1 (Select mode), the request does not contain an M24LR64E-R Unique ID. The M24LR64E-R in the Selected state that receives a request with the Select_flag set to 1 executes it and returns a response to the VCD as specified in the command description.

Only M24LR64E-Rs in the Selected state answer a request where the Select_flag is set to 1.

The system design ensures in theory that only one M24LR64E-R can be in the Select state at any given time.

19 Request format

The request consists of:

- an SOF,
- flags,
- a command code,
- parameters and data,
- a CRC,
- an EOF.

Table 26. General request format

SOF	Request_flags	Command code	Parameters	Data	CRC	EOF

19.1 Request flags

In a request, the “flags” field specifies the actions to be performed by the M24LR64E-R and whether corresponding fields are present or not.

The flags field consists of eight bits. Bit 3 (Inventory_flag) of the request flag defines the contents of the four MSBs (bits 5 to 8). When bit 3 is reset (0), bits 5 to 8 define the M24LR64E-R selection criteria. When bit 3 is set (1), bits 5 to 8 define the M24LR64E-R Inventory parameters.

Table 27. Definition of request flags 1 to 4

Bit No.	Flag	Level	Description
Bit 1	Subcarrier_flag(1)	0	A single subcarrier frequency is used by the M24LR64E-R
		1	Two subcarriers are used by the M24LR64E-R
Bit 2	Data_rate_flag(2)	0	Low data rate is used
		1	High data rate is used
Bit 3	Inventory_flag	0	The meaning of flags 5 to 8 is described in *Table 28*
		1	The meaning of flags 5 to 8 is described in *Table 29*
Bit 4	Protocol_extension_flag(3)	0	No Protocol format extension
		1	Protocol format extension

1. Subcarrier_flag refers to the M24LR64E-R-to-VCD communication.
2. Data_rate_flag refers to the M24LR64E-R-to-VCD communication.
3. Protocol_extension_flag must be set to 1 for Read Single Block, Read Multiple Block, Fast Read Multiple Block, Write Single Block, and Get Multiple Block Security Status commands. Get System Info command supports two options: a standard response format when Protocol_extension_flag is set to 0, and a rich response when protocol extension is set to 1.

Table 28. Request flags 5 to 8 when Bit 3 = 0

Bit No.	Flag	Level	Description
Bit 5	Select flag(1)	0	The request is executed by any M24LR64E-R according to the setting of Address_flag
		1	The request is executed only by the M24LR64E-R in Selected state
Bit 6	Address flag(1)	0	The request is not addressed. UID field is not present. The request is executed by all M24LR64E-Rs.
		1	The request is addressed. UID field is present. The request is executed only by the M24LR64E-R whose UID matches the UID specified in the request.
Bit 7	Option flag	0	Option not activated.
		1	Option activated.
Bit 8	RFU	0	-

1. If the Select_flag is set to 1, the Address_flag is set to 0 and the UID field is not present in the request.

Table 29. Request flags 5 to 8 when Bit 3 = 1

Bit No.	Flag	Level	Description
Bit 5	AFI flag	0	AFI field is not present
		1	AFI field is present
Bit 6	Nb_slots flag	0	16 slots
		1	1 slot
Bit 7	Option flag	0	-
Bit 8	RFU	0	-

20 Response format

The response consists of:

- an SOF,
- flags,
- parameters and data,
- a CRC,
- an EOF.

Table 30. General response format

SOF	Response_flags	Parameters	Data	CRC	EOF

20.1 Response flags

In a response, the flags indicate how actions have been performed by the M24LR64E-R and whether corresponding fields are present or not. The response flags consist of eight bits.

Table 31. Definitions of response flags 1 to 8

Bit No.	Flag	Level	Description
Bit 1	Error_flag	0	No error
		1	Error detected. Error code is in the “Error” field.
Bit 2	RFU	0	-
Bit 3	RFU	0	-
Bit 4	Extension flag	0	No extension
Bit 5	RFU	0	-
Bit 6	RFU	0	-
Bit 7	RFU	0	-
Bit 8	RFU	0	-

20.2 Response error code

If the Error_flag is set by the M24LR64E-R in the response, the Error code field is present and provides information about the error that occurred.

Error codes not specified in *Table 32* are reserved for future use.

Table 32. Response error code definition

Error code	Meaning
03h	The option is not supported.
0Fh	Error with no information given.
10h	The specified block is not available.
11h	The specified block is already locked and thus cannot be locked again.
12h	The specified block is locked and its contents cannot be changed.
13h	The specified block was not successfully programmed.
14h	The specified block was not successfully locked.
15h	The specified block is read-protected.

21 Anticollision

The purpose of the anticollision sequence is to inventory the M24LR64E-Rs present in the VCD field using their unique ID (UID).

The VCD is the master of communications with one or several M24LR64E-Rs. It initiates an M24LR64E-R communication by issuing the Inventory request.

The M24LR64E-R sends its response in the determined slot or does not respond.

21.1 Request parameters

When issuing the Inventory Command:

- The VCD sets the Nb_slots_flag as desired.
- The VCD adds the mask length and the mask value after the command field:
  - The mask length is the number of significant bits of the mask value.
  - The mask value is contained in an integer number of bytes. The mask length indicates the number of significant bits. LSB is transmitted first.
- If the mask length is not a multiple of 8 (bits), as many 0-bits as required are added to the mask value MSB, so that the mask value is contained in an integer number of bytes.
- The next field starts at the next byte boundary.

Table 33. Inventory request format

MSB LSB

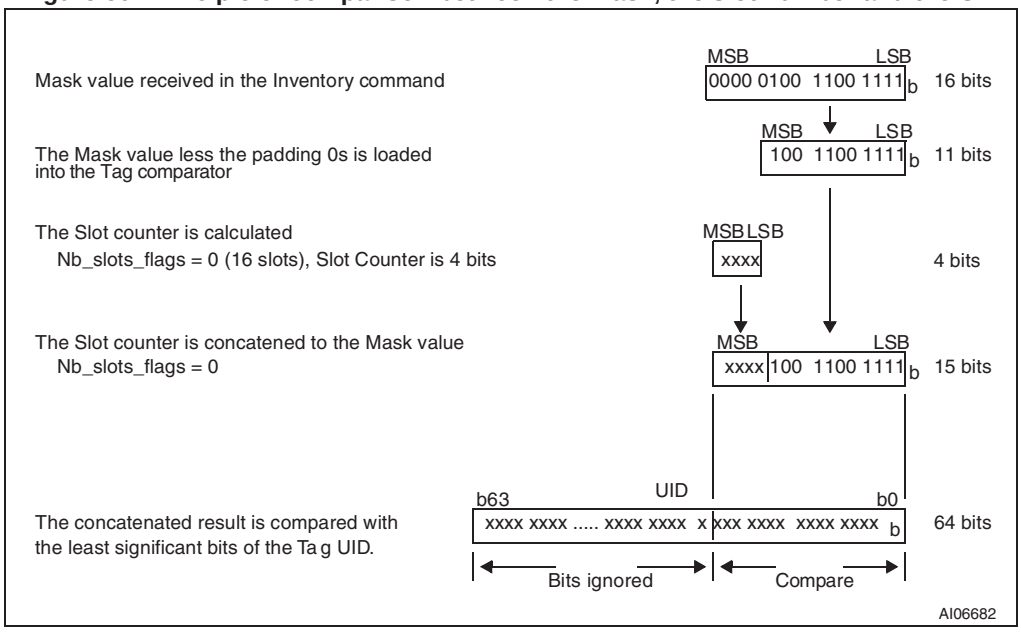
SOF	Request_flags	Command	Optional AFI	Mask length	Mask value	CRC	EOF
-	8 bits	8 bits	8 bits	8 bits	0 to 8 bytes	16 bits	-

In the example provided in *Table 34* and *Figure 50*, the mask length is 11 bits. Five 0-bits are added to the mask value MSB. The 11-bit mask and the current slot number are compared to the UID.

Table 34. Example of the addition of 0-bits to an 11-bit mask value

MSB (b_{15})	LSB (b_0)
0000 0	100 1100 1111
0-bits added	11-bit mask value

Figure 50. Principle of comparison between the mask, the slot number and the UID



The AFI field is present if the AFI_flag is set.

The pulse is generated according to the definition of the EOF in ISO/IEC 15693-2.

The first slot starts immediately after the request EOF is received. To switch to the next slot, the VCD sends an EOF.

The following rules and restrictions apply:

- If no M24LR64E-R answer is detected, the VCD may switch to the next slot by sending an EOF.
- If one or more M24LR64E-R answers are detected, the VCD waits until the complete frame has been received before sending an EOF for switching to the next slot.

22 Request processing by the M24LR64E-R

Upon reception of a valid request, the M24LR64E-R performs the following algorithm:

- NbS is the total number of slots (1 or 16)
- SN is the current slot number (0 to 15)
- LSB (value, n) function returns the n Less Significant Bits of value
- MSB (value, n) function returns the n Most Significant Bits of value
- “&” is the concatenation operator
- Slot_Frame is either an SOF or an EOF

```
SN = 0
if (Nb_slots_flag)
   then NbS = 1
        SN_length = 0
        endif
   else NbS = 16
        SN_length = 4
        endif

label1:
if LSB(UID, SN_length + Mask_length) =
  LSB(SN,SN_length)&LSB(Mask,Mask_length)
   then answer to inventory request
        endif

wait (Slot_Frame)

if Slot_Frame = SOF
   then Stop Anticollision
        decode/process request
        exit
        endif

if Slot_Frame = EOF
   if SN < NbS-1
      then SN = SN + 1
           goto label1
           exit
           endif
   endif
```

23 Explanation of the possible cases

Figure 51 summarizes the main possible cases that can occur during an anticollision sequence when the number of slots is 16.

The sequence of steps is as follows:

- The VCD sends an Inventory request, in a frame terminated by an EOF. The number of slots is 16.
- M24LR64E-R_1 transmits its response in Slot 0. It is the only one to do so, therefore no collision occurs and its UID is received and registered by the VCD.
- The VCD sends an EOF in order to switch to the next slot.
- In Slot 1, two M24LR64E-Rs (M24LR64E-R_2 and M24LR64E-R_3) transmit a response, thus generating a collision. The VCD records the event and registers that a collision was detected in Slot 1.
- The VCD sends an EOF in order to switch to the next slot.
- In Slot 2, no M24LR64E-R transmits a response. Therefore the VCD does not detect any M24LR64E-R SOF and switches to the next slot by sending an EOF.
- In Slot 3, another collision occurs due to responses from M24LR64E-R_4 and M24LR64E-R_5.
- The VCD sends a request (for instance a Read Block) to M24LR64E-R_1 whose UID has already been correctly received.
- All M24LR64E-Rs detect an SOF and exit the anticollision sequence. They process this request and since the request is addressed to M24LR64E-R_1, only M24LR64E-R_1 transmits a response.
- All M24LR64E-Rs are ready to receive another request. If it is an Inventory command, the slot numbering sequence restarts from 0.

Note: The decision to interrupt the anticollision sequence is made by the VCD. EOFs could have been sent until Slot 16, and the request to M24LR64E-R_1 sent then.

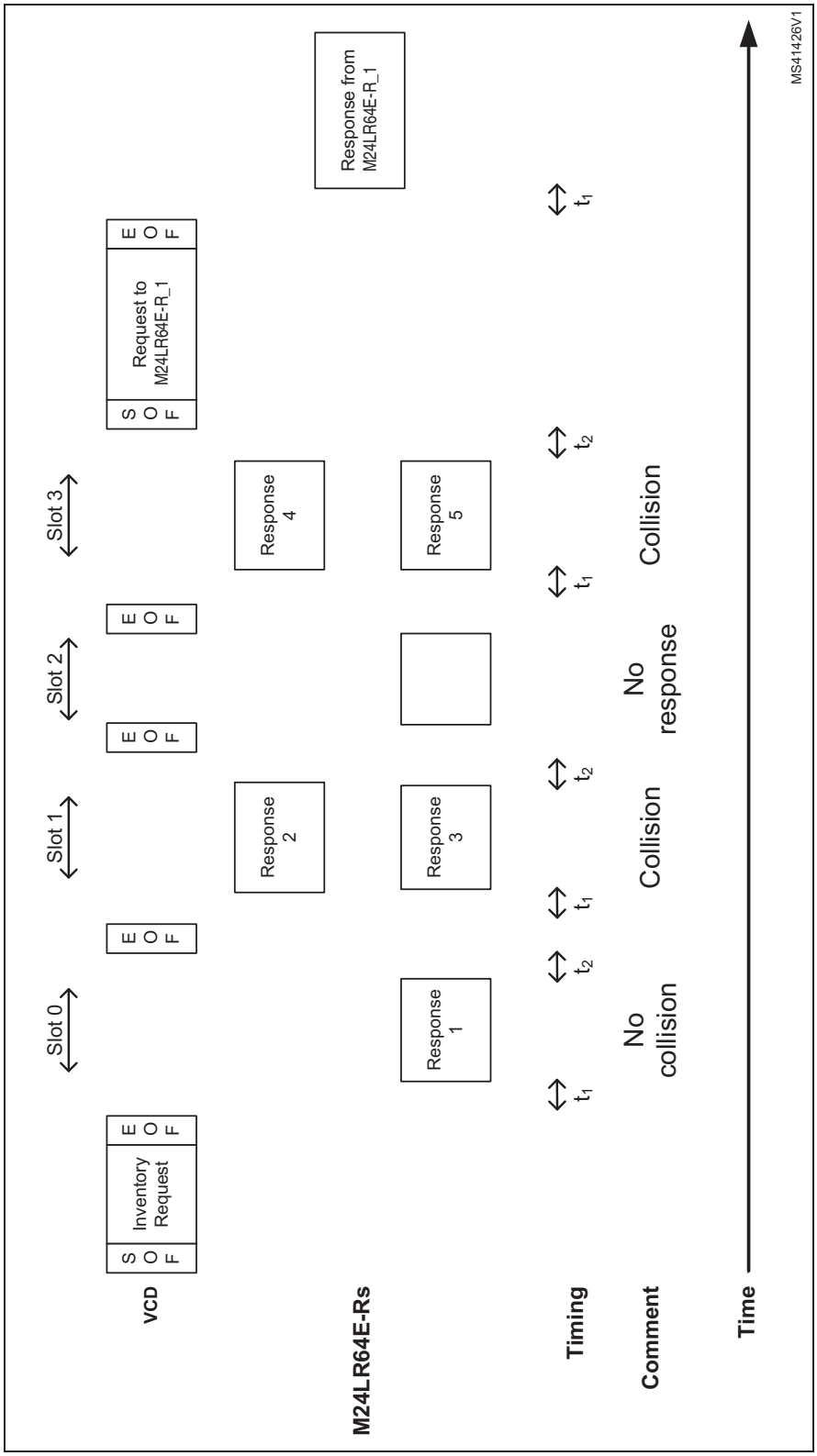


Figure 51. Description of a possible anticollision sequence

24 Inventory Initiated command

The M24LR64E-R provides a special feature to improve the inventory time response of moving tags using the Initiate_flag value. This flag, controlled by the Initiate command, allows tags to answer Inventory Initiated commands.

For applications in which multiple tags are moving in front of a reader, it is possible to miss tags using the standard inventory command. The reason is that the inventory sequence has to be performed on a global tree search. For example, a tag with a particular UID value may have to wait the run of a long tree search before being inventoried. If the delay is too long, the tag may be out of the field before it has been detected.

Using the Initiate command, the inventory sequence is optimized. When multiple tags are moving in front of a reader, the ones which are within the reader field are initiated by the Initiate command. In this case, a small batch of tags answers to the Inventory Initiated command, which optimizes the time necessary to identify all the tags. When finished, the reader has to issue a new Initiate command in order to initiate a new small batch of tags which are new inside the reader field.

It is also possible to reduce the inventory sequence time using the Fast Initiate and Fast Inventory Initiated commands. These commands allow the M24LR64E-Rs to increase their response data rate by a factor of 2, up to 53 Kbit/s.

25 Timing definition

25.1 t_1: M24LR64E-R response delay

Upon detection of the rising edge of the EOF received from the VCD, the M24LR64E-R waits for a t_{1nom} time before transmitting its response to a VCD request or switching to the next slot during an inventory process. Values of t_1 are given in *Table 35*. The EOF is defined in *Figure 22*.

25.2 t_2: VCD new request delay

t_2 is the time after which the VCD may send an EOF to switch to the next slot when one or more M24LR64E-R responses have been received during an Inventory command. It starts from the reception of the EOF from the M24LR64E-Rs.

The EOF sent by the VCD may be either 10% or 100% modulated regardless of the modulation index used for transmitting the VCD request to the M24LR64E-R.

t_2 is also the time after which the VCD may send a new request to the M24LR64E-R, as described in *Figure 48*.

Values of t_2 are given in *Table 35*.

25.3 t_3: VCD new request delay when no response is received from the M24LR64E-R

t_3 is the time after which the VCD may send an EOF to switch to the next slot when no M24LR64E-R response has been received.

The EOF sent by the VCD may be either 10% or 100% modulated regardless of the modulation index used for transmitting the VCD request to the M24LR64E-R.

From the time the VCD has generated the rising edge of an EOF:

- If this EOF is 100% modulated, the VCD waits for a time at least equal to t_{3min} before sending a new EOF.
- If this EOF is 10% modulated, the VCD waits for a time at least equal to the sum of t_{3min} + the M24LR64E-R nominal response time (which depends on the M24LR64E-R data rate and subcarrier modulation mode) before sending a new EOF.

Table 35. Timing values(1)

	Minimum (min) values	Nominal (nom) values	Maximum (max) values
t_1	318.6 µs	320.9 µs	323.3 µs
t_2	309.2 µs	No t_{nom}	No t_{max}
t_3	t_{1max}(2) + t_{SOF}(3)	No t_{nom}	No t_{max}

1. The tolerance of specific timings is ± 32/fC.
2. t_{1max} does not apply for write-alike requests. Timing conditions for write-alike requests are defined in the command description.
3. t_{SOF} is the time taken by the M24LR64E-R to transmit an SOF to the VCD. t_{SOF} depends on the current data rate: High data rate or Low data rate.

26 Command codes

The M24LR64E-R supports the commands described in this section. Their codes are given in *Table 36*.

Table 36. Command codes

Command code standard	Function	Command code custom	Function
01h	Inventory	2Ch	Get Multiple Block Security Status
02h	Stay Quiet	B1h	Write-sector Password
20h	Read Single Block	B2h	Lock-sector
21h	Write Single Block	B3h	Present-sector Password
23h	Read Multiple Block	C0h	Fast Read Single Block
25h	Select	C1h	Fast Inventory Initiated
26h	Reset to Ready	C2h	Fast Initiate
27h	Write AFI	C3h	Fast Read Multiple Block
28h	Lock AFI	D1h	Inventory Initiated
29h	Write DSFID	D2h	Initiate
2Ah	Lock DSFID	A0h	ReadCfg
2Bh	Get System Info	A1h	WriteEHCfg
-	-	A2h	SetRstEHEn
-	-	A3h	CheckEHEn
-	-	A4h	WriteDOCfg

26.1 Inventory

When receiving the Inventory request, the M24LR64E-R runs the anticollision sequence. The Inventory_flag is set to 1. The meaning of flags 5 to 8 is shown in *Table 29*.

The request contains:

- the flags,
- the Inventory command code (see *Table 36*),
- the AFI if the AFI flag is set,
- the mask length,
- the mask value,
- the CRC.

The M24LR64E-R does not generate any answer in case of error.

Table 37. Inventory request format

Request SOF	Request_flags	Inventory	Optional AFI	Mask length	Mask value	CRC16	Request EOF
-	8 bits	01h	8 bits	8 bits	0 - 64 bits	16 bits	-

The response contains:

- the flags,
- the Unique ID.

Table 38. Inventory response format

Response SOF	Response_flags	DSFID	UID	CRC16	Response EOF
-	8 bits	8 bits	64 bits	16 bits	-

During an Inventory process, if the VCD does not receive an RF M24LR64E-R response, it waits for a time t_3 before sending an EOF to switch to the next slot. t_3 starts from the rising edge of the request EOF sent by the VCD.

- If the VCD sends a 100% modulated EOF, the minimum value of t_3 is:
  $t_3 min = 4384/f_C$ (323.3µs) + t_{SOF}
- If the VCD sends a 10% modulated EOF, the minimum value of t_3 is:
  $t_3 min = 4384/f_C$ (323.3µs) + t_{NRT}

where:

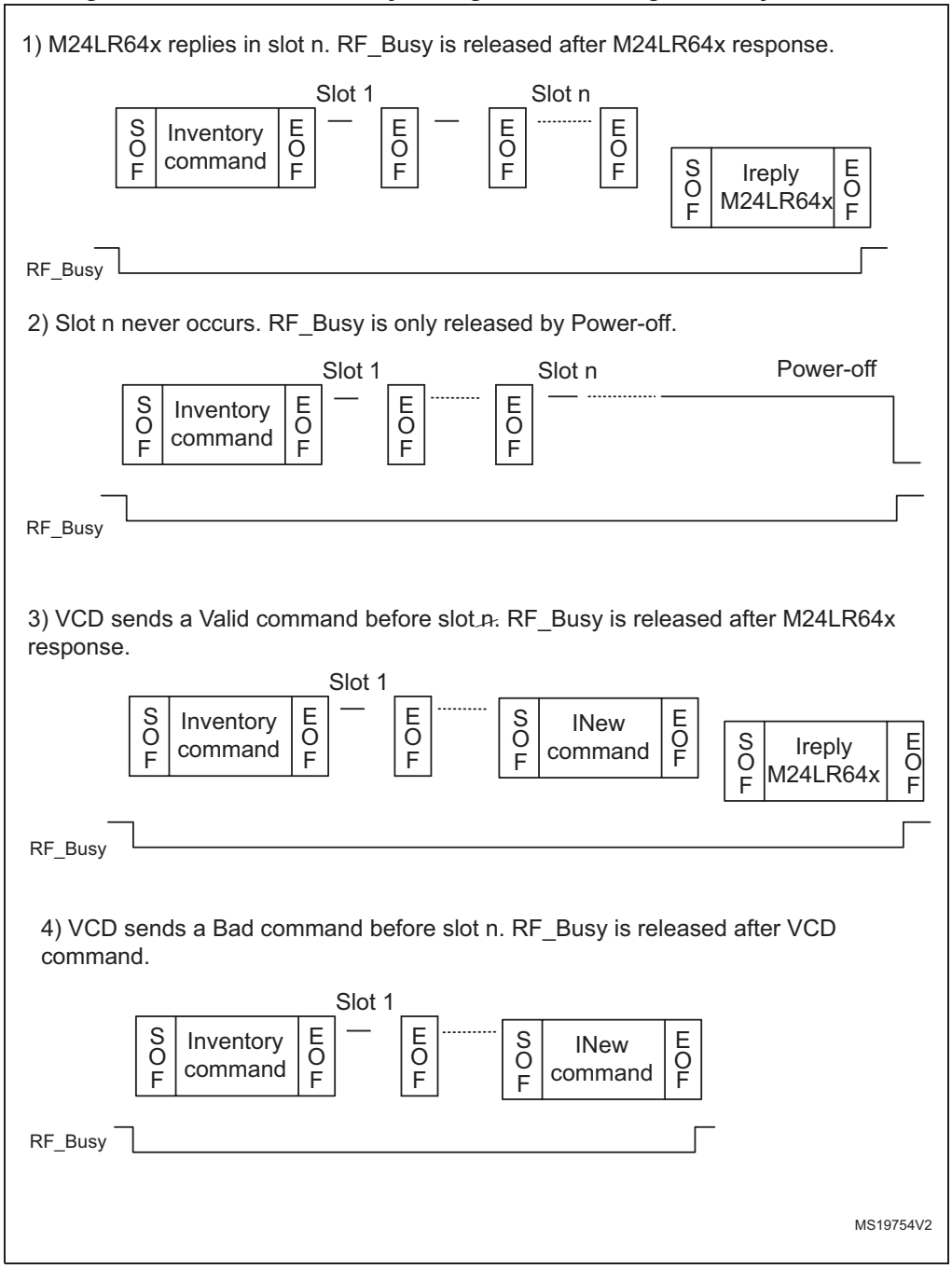
- t_{SOF} is the time required by the M24LR64E-R to transmit an SOF to the VCD,
- t_{NRT} is the nominal response time of the M24LR64E-R.

t_{NRT} and t_{SOF} are dependent on the M24LR64E-R-to-VCD data rate and subcarrier modulation mode.

When configured in the RF busy mode, the RF WIP/BUSY pin is tied to 0 from the SOF starting the inventory command to the end of the M24LR64E-R response. If the M24LR64E-R does not receive the corresponding slot marker, the RF WIP/BUSY pin remains at 0 until the next RF power-off.

When configured in the RF write in progress mode, the RF WIP/BUSY pin remains in high-Z state.

Figure 52. M24LR64E RF-Busy management following Inventory command



26.2 Stay Quiet

Command code = 0x02

On receiving the Stay Quiet command, the M24LR64E-R enters the Quiet state if no error occurs, and does NOT send back a response. There is NO response to the Stay Quiet command even if an error occurs.

When in the Quiet state:

- the M24LR64E-R does not process any request if the Inventory_flag is set,
- the M24LR64E-R processes any Addressed request.

The M24LR64E-R exits the Quiet state when:

- it is reset (power off),
- receiving a Select request. It then goes to the Selected state,
- receiving a Reset to Ready request. It then goes to the Ready state.

Table 39. Stay Quiet request format

Request SOF	Request flags	Stay Quiet	UID	CRC16	Request EOF
-	8 bits	02h	64 bits	16 bits	-

The Stay Quiet command must always be executed in Addressed mode (Select_flag is reset to 0 and Address_flag is set to 1).

Figure 53. Stay Quiet frame exchange between VCD and M24LR64E-R

When configured in the RF busy mode, the RF WIP/BUSY pin is tied to 0 during the Stay Quiet command.

When configured in the RF write in progress mode, the RF WIP/BUSY pin remains in high-Z state.

26.3 Read Single Block

On receiving the Read Single Block command, the M24LR64E-R reads the requested block and sends back its 32-bit value in the response. The Protocol_extension_flag should be set to 1 for the M24LR64E-R to operate correctly. If the Protocol_extension_flag is at 0, the M24LR64E-R answers with an error code. The Option_flag is supported.

Table 40. Read Single Block request format

Request SOF	Request_flags	Read Single Block	UID(1)	Block number	CRC16	Request EOF
-	8 bits	20h	64 bits	16 bits	16 bits	-

1. Gray color means that the field is optional.

Request parameters:

- Request flags
- UID (optional)
- Block number

Table 41. Read Single Block response format when Error_flag is NOT set

Response SOF	Response_flags	Sector security status(1)	Data	CRC16	Response EOF
-	8 bits	8 bits	32 bits	16 bits	-

1. Gray color means that the field is optional.

Response parameters:

- Sector security status if Option_flag is set (see *Table 42*)
- Four bytes of block data

Table 42. Sector security status

b_7	b_6	b_5	b_4	b_3	b_2	b_1	b_0
Reserved for future use. All at 0.			Password control bits		Read / Write protection bits		0: Current sector not locked 1: Current sector locked

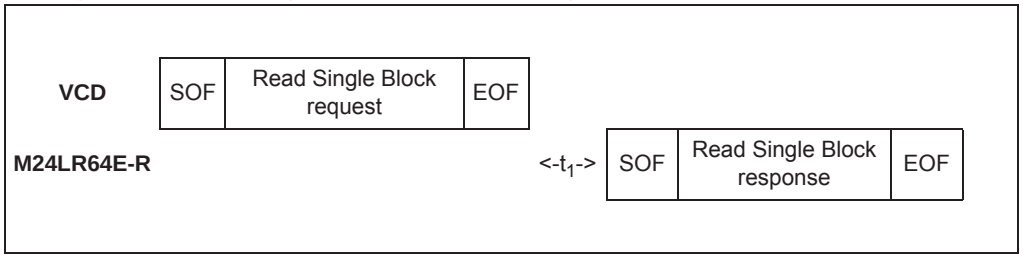
Table 43. Read Single Block response format when Error_flag is set

Response SOF	Response_flags	Error code	CRC16	Response EOF
-	8 bits	8 bits	16 bits	-

Response parameter:

- Error code as Error_flag is set
  - 10h: the specified block is not available
  - 15h: the specified block is read-protected

Figure 54. Read Single Block frame exchange between VCD and M24LR64E-R



When configured in the RF busy mode, the RF WIP/BUSY pin is tied to 0 from the SOF that starts the Read Single Block command to the end of the M24LR64E-R response.

When configured in the RF write in progress mode, the RF WIP/BUSY pin remains in high-Z state.

26.4 Write Single Block

On receiving the Write Single Block command, the M24LR64E-R writes the data contained in the request to the requested block and reports whether the write operation was successful in the response. The Protocol_extension_flag should be set to 1 for the M24LR64E-R to operate correctly. If the Protocol_extension_flag is at 0, the M24LR64E-R answers with an error code. The Option_flag is supported.

During the RF write cycle W_t, there should be no modulation (neither 100% nor 10%), otherwise the M24LR64E-R may not program correctly the data into the memory. The W_t time is equal to t_{1nom} + 18 × 302 µs.

Table 44. Write Single Block request format

Request SOF	Request_flags	Write Single Block	UID(1)	Block number	Data	CRC16	Request EOF
-	8 bits	21h	64 bits	16 bits	32 bits	16 bits	-

1. Gray color means that the field is optional.

Request parameters:

- Request flags
- UID (optional)
- Block number
- Data

Table 45. Write Single Block response format when Error_flag is NOT set

Response SOF	Response_flags	CRC16	Response EOF
-	8 bits	16 bits	-

Response parameter:

- No parameter. The response is sent back after the writing cycle.

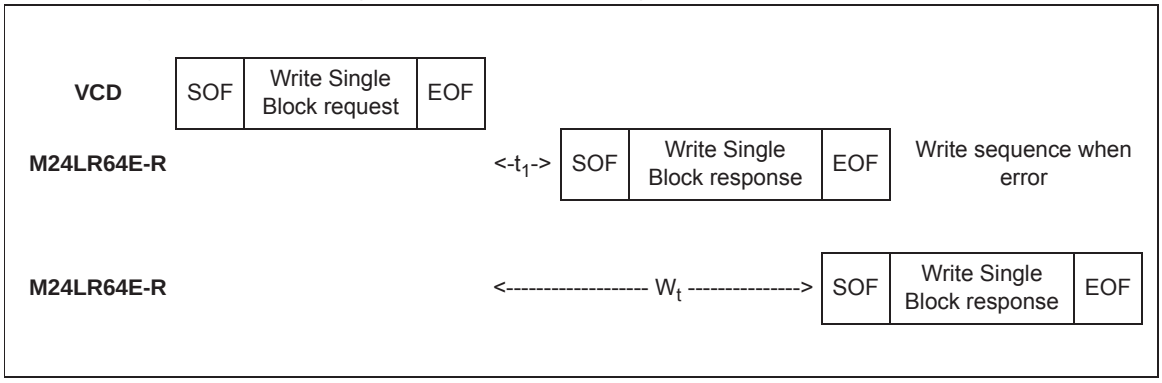
Table 46. Write Single Block response format when Error_flag is set

Response SOF	Response_flags	Error code	CRC16	Response EOF
-	8 bits	8 bits	16 bits	-

Response parameter:

- Error code as Error_flag is set:
  - 0Fh: error with no information given
  - 10h: the specified block is not available
  - 12h: the specified block is locked and its contents cannot be changed
  - 13h: the specified block was not successfully programmed

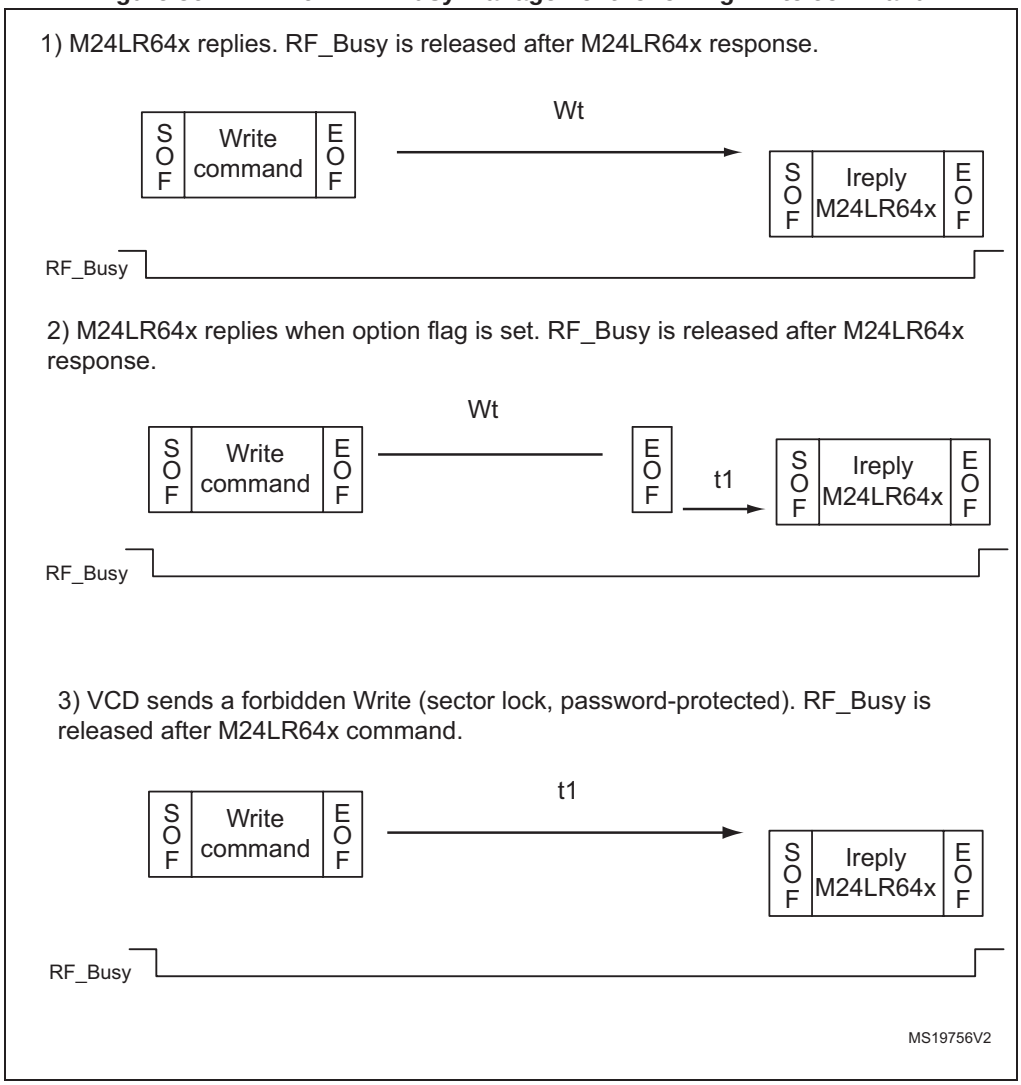
Figure 55. Write Single Block frame exchange between VCD and M24LR64E-R



When configured in the RF busy mode, the RF WIP/BUSY pin is tied to 0 from the SOF that starts the Write Single Block command to the end of the M24LR64E-R response.

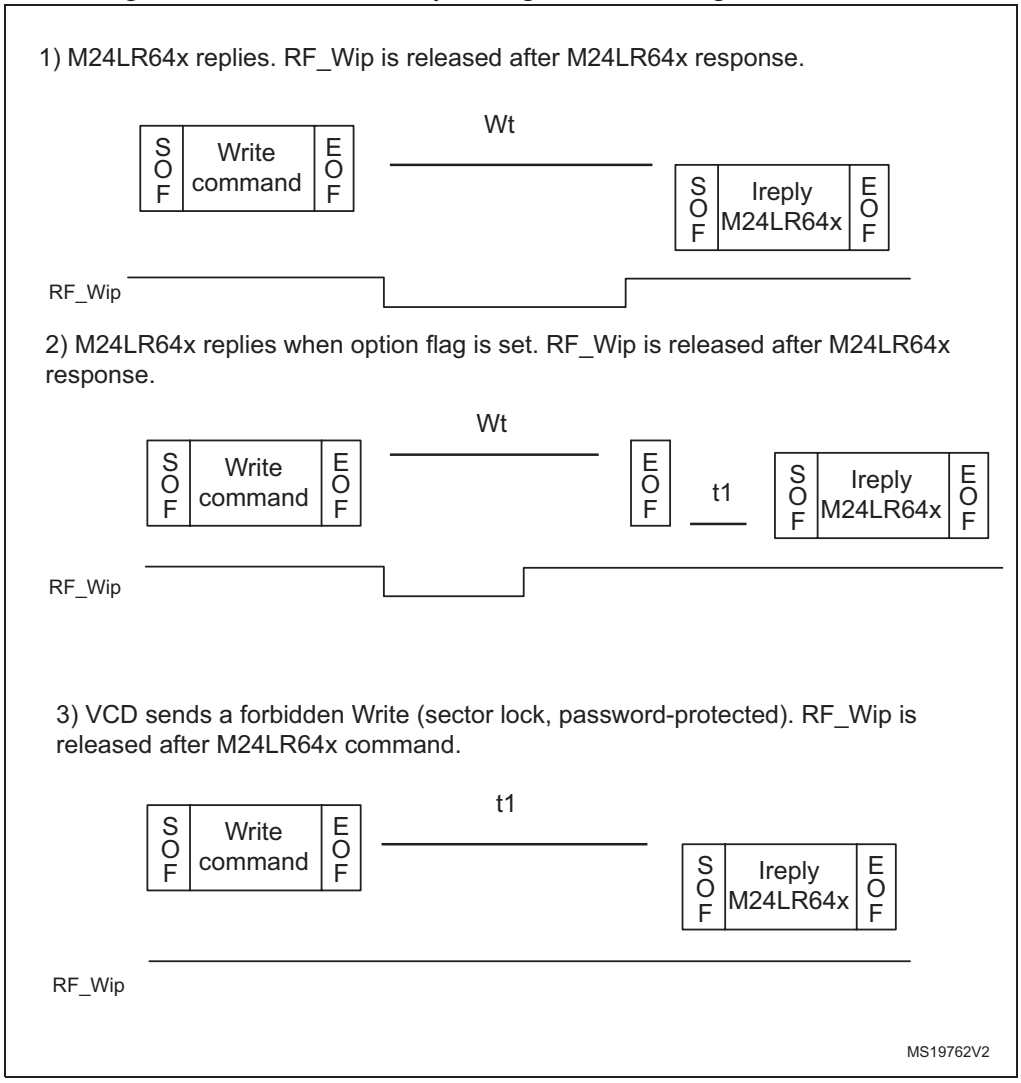
When configured in the RF write in progress mode, the RF WIP/BUSY pin is tied to 0 for the duration of the internal write cycle (from the end of a valid write single block command to the beginning of the M24LR64E-R response).

Figure 56. M24LR64E RF-Busy management following Write command



When configuring in the RF Write in progress mode, the RF WIP/BUSY pin is tied to 0 during the Write & verify sequence, as shown in *Figure 57*.

Figure 57. M24LR64E RF-Wip management following Write command



26.5 Read Multiple Block

When receiving the Read Multiple Block command, the M24LR64E-R reads the selected blocks and sends back their value in multiples of 32 bits in the response. The blocks are numbered from 00h to 1FFh in the request and the value is minus one (–1) in the field. For example, if the “Number of blocks” field contains the value 06h, seven blocks are read. The maximum number of blocks is fixed at 32 assuming that they are all located in the same sector. If the number of blocks overlaps sectors, the M24LR64E-R returns an error code.

The Protocol_extension_flag should be set to 1 for the M24LR64E-R to operate correctly. If the Protocol_extension_flag is at 0, the M24LR64E-R answers with an error code. The Option_flag is supported.

Table 47. Read Multiple Block request format

Request SOF	Request_ flags	Read Multiple Block	UID(1)	First block number	Number of blocks	CRC16	Request EOF
-	8 bits	23h	64 bits	16 bits	8 bits	16 bits	-

1. Gray color means that the field is optional.

Request parameters:

- Request flags
- UID (optional)
- First block number
- Number of blocks

Table 48. Read Multiple Block response format when Error_flag is NOT set

Response SOF	Response_ flags	Sector security status(1)	Data	CRC16	Response EOF
-	8 bits	8 bits(2)	32 bits(2)	16 bits	-

1. Gray color means that the field is optional.
2. Repeated as needed.

Response parameters:

- Sector security status if Option_flag is set (see *Table 49*)
- N blocks of data

Table 49. Sector security status

b_7 b_6	b_5 b_4 b_3	b_2 b_1	b_0
Reserved for future use. All at 0.	Password control bits	Read / Write protection bits	0: Current sector not locked 1: Current sector locked

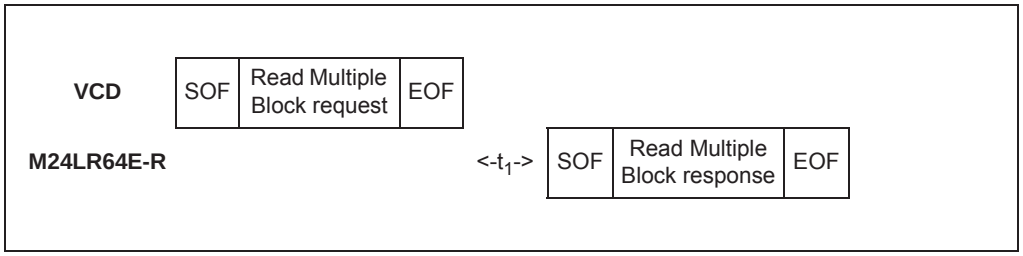
Table 50. Read Multiple Block response format when Error_flag is set

Response SOF	Response_flags	Error code	CRC16	Response EOF
-	8 bits	8 bits	16 bits	-

Response parameter:

- Error code as Error_flag is set:
  - 0Fh: error with no information given
  - 10h: the specified block is not available
  - 15h: the specified block is read-protected

Figure 58. Read Multiple Block frame exchange between VCD and M24LR64E-R



When configured in the RF busy mode, the RF WIP/BUSY pin is tied to 0 from the SOF that starts the Read Multiple Block command to the end of the M24LR64E-R response.

When configured in the RF write in progress mode, the RF WIP/BUSY pin remains in high-Z state.

26.6 Select

When receiving the Select command:

- If the UID is equal to its own UID, the M24LR64E-R enters or stays in the Selected state and sends a response.
- If the UID does not match its own UID, the selected M24LR64E-R returns to the Ready state and does not send a response.

The M24LR64E-R answers an error code only if the UID is equal to its own UID. If not, no response is generated. If an error occurs, the M24LR64E-R remains in its current state.

Table 51. Select request format

Request SOF	Request_flags	Select	UID	CRC16	Request EOF
-	8 bits	25h	64 bits	16 bits	-

Request parameter:

- UID

Table 52. Select Block response format when Error_flag is NOT set

Response SOF	Response_flags	CRC16	Response EOF
-	8 bits	16 bits	-

Response parameter:

- No parameter

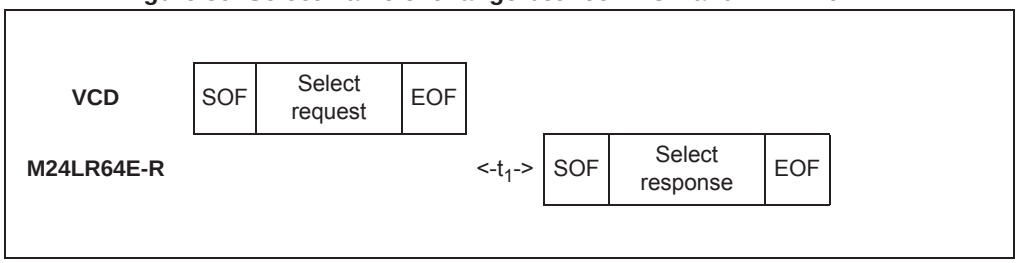
Table 53. Select response format when Error_flag is set

Response SOF	Response_flags	Error code	CRC16	Response EOF
-	8 bits	8 bits	16 bits	-

Response parameter:

- Error code as Error_flag is set:
  - 03h: the option is not supported

Figure 59. Select frame exchange between VCD and M24LR64E-R



When configured in the RF busy mode, the RF WIP/BUSY pin is tied to 0 from the SOF that starts the Select command to the end of the M24LR64E-R response.

When configured in the RF write in progress mode, the RF WIP/BUSY pin remains in high-Z state.

26.7 Reset to Ready

On receiving a Reset to Ready command, the M24LR64E-R returns to the Ready state if no error occurs. In the Addressed mode, the M24LR64E-R answers an error code only if the UID is equal to its own UID. If not, no response is generated.

Table 54. Reset to Ready request format

Request SOF	Request_flags	Reset to Ready	UID(1)	CRC16	Request EOF
-	8 bits	26h	64 bits	16 bits	-

1. Gray color means that the field is optional.

Request parameter:

- UID (optional)

Table 55. Reset to Ready response format when Error_flag is NOT set

Response SOF	Response_flags	CRC16	Response EOF
-	8 bits	16 bits	-

Response parameter:

- No parameter

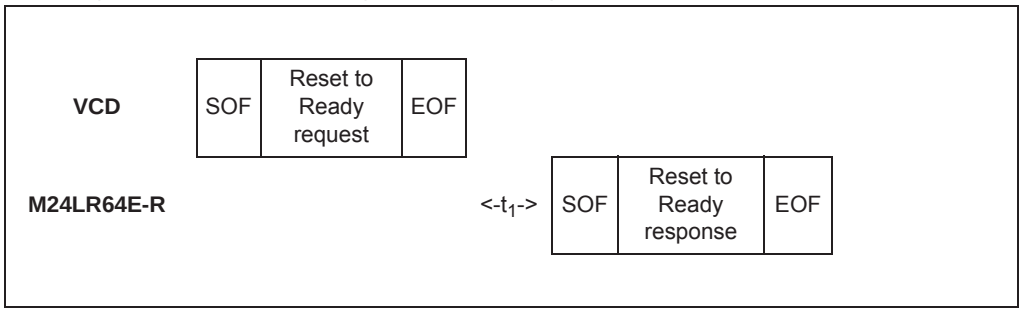
Table 56. Reset to ready response format when Error_flag is set

Response SOF	Response_flags	Error code	CRC16	Response EOF
-	8 bits	8 bits	16 bits	-

Response parameter:

- Error code as Error_flag is set:
  - 03h: the option is not supported

Figure 60. Reset to Ready frame exchange between VCD and M24LR64E-R



When configured in the RF busy mode, the RF WIP/BUSY pin is tied to 0 from the SOF that starts the Reset to ready command to the end of the M24LR64E-R response.

When configured in the RF write in progress mode, the RF WIP/BUSY pin remains in high-Z state.

26.8 Write AFI

On receiving the Write AFI request, the M24LR64E-R programs the 8-bit AFI value to its memory. The Option_flag is supported.

During the RF write cycle W_t, there should be no modulation (neither 100% nor 10%), otherwise the M24LR64E-R may not write correctly the AFI value into the memory. The W_t time is equal to t_{1nom} + 18 × 302 µs.

Table 57. Write AFI request format

Request SOF	Request_flags	Write AFI	UID(1)	AFI	CRC16	Request EOF
-	8 bits	27h	64 bits	8 bits	16 bits	-

1. Gray color means that the field is optional.

Request parameter:

- Request flags
- UID (optional)
- AFI

Table 58. Write AFI response format when Error_flag is NOT set

Response SOF	Response_flags	CRC16	Response EOF
-	8 bits	16 bits	-

Response parameter:

- No parameter

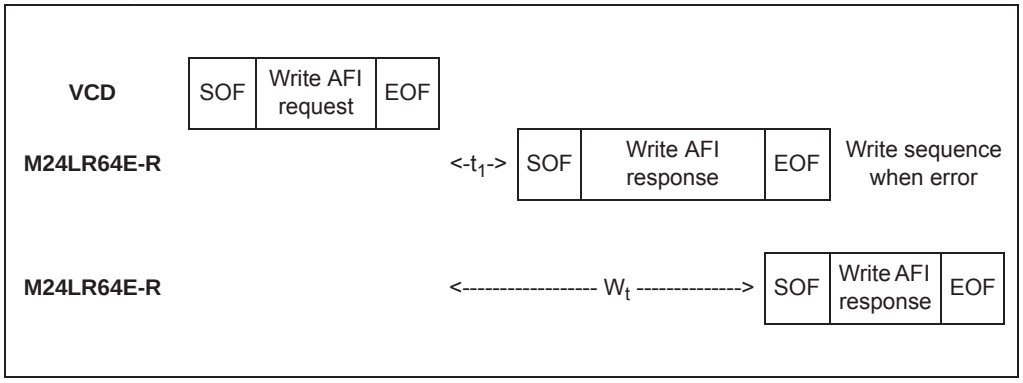
Table 59. Write AFI response format when Error_flag is set

Response SOF	Response_ flags	Error code	CRC16	Response EOF
-	8 bits	8 bits	16 bits	-

Response parameter:

- Error code as Error_flag is set
  - 12h: the specified block is locked and its contents cannot be changed
  - 13h: the specified block was not successfully programmed

Figure 61. Write AFI frame exchange between VCD and M24LR64E-R



When configured in the RF busy mode, the RF WIP/BUSY pin is tied to 0 from the SOF that starts the Write AFI command to the end of the M24LR64E-R response.

When configured in the RF write in progress mode, the RF WIP/BUSY pin is tied to 0 for the duration of the internal write cycle (from the end of a valid Write AFI command to the beginning of the M24LR64E-R response).

26.9 Lock AFI

On receiving the Lock AFI request, the M24LR64E-R locks the AFI value permanently. The Option_flag is supported.

During the RF write cycle W_t, there should be no modulation (neither 100% nor 10%), otherwise the M24LR64E-R may not lock correctly the AFI value in memory. The W_t time is equal to t_{1nom} + 18 × 302 µs.

Table 60. Lock AFI request format

Request SOF	Request_flags	Lock AFI	UID(1)	CRC16	Request EOF
-	8 bits	28h	64 bits	16 bits	-

1. Gray color means that the field is optional.

Request parameter:

- Request Flags
- UID (optional)

Table 61. Lock AFI response format when Error_flag is NOT set

Response SOF	Response_flags	CRC16	Response EOF
-	8 bits	16 bits	-

Response parameter:

- No parameter

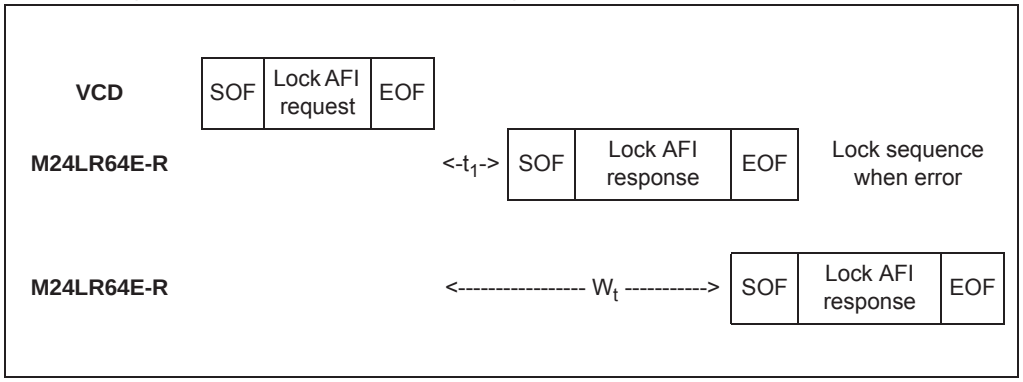
Table 62. Lock AFI response format when Error_flag is set

Response SOF	Response_flags	Error code	CRC16	Response EOF
-	8 bits	8 bits	16 bits	-

Response parameter:

- Error code as Error_flag is set
  - 11h: the specified block is already locked and thus cannot be locked again
  - 14h: the specified block was not successfully locked

Figure 62. Lock AFI frame exchange between VCD and M24LR64E-R



When configured in the RF busy mode, the RF WIP/BUSY pin is tied to 0 from the SOF that starts the Lock AFI command to the end of the M24LR64E-R response.

When configured in the RF write in progress mode, the RF WIP/BUSY pin is tied to 0 for the entire duration of the internal write cycle (from the end of valid Lock AFI command to the beginning of the M24LR64E-R response).

26.10 Write DSFID

On receiving the Write DSFID request, the M24LR64E-R programs the 8-bit DSFID value to its memory. The Option_flag is supported.

During the RF write cycle W_t, there should be no modulation (neither 100% nor 10%), otherwise the M24LR64E-R may not write correctly the DSFID value in memory. The W_t time is equal to t_{1nom} + 18 × 302 µs.

Table 63. Write DSFID request format

Request SOF	Request_flags	Write DSFID	UID(1)	DSFID	CRC16	Request EOF
-	8 bits	29h	64 bits	8 bits	16 bits	-

1. Gray color means that the field is optional.

Request parameter:

- Request flags
- UID (optional)
- DSFID

Table 64. Write DSFID response format when Error_flag is NOT set

Response SOF	Response_flags	CRC16	Response EOF
-	8 bits	16 bits	-

Response parameter:

- No parameter

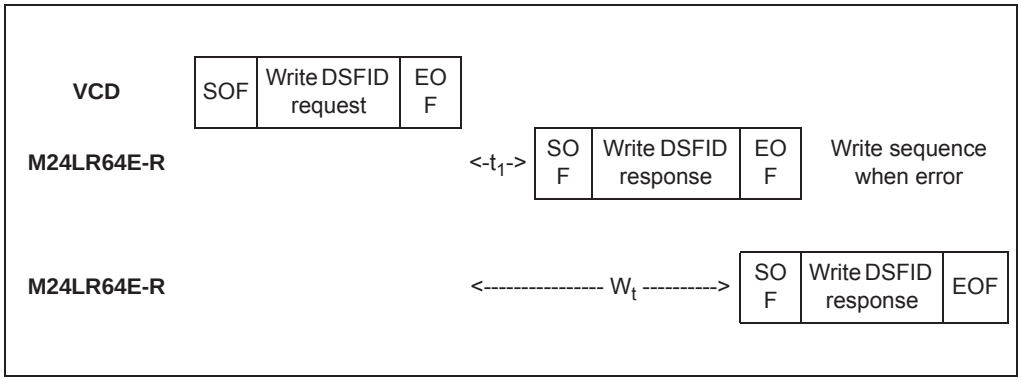
Table 65. Write DSFID response format when Error_flag is set

Response SOF	Response_flags	Error code	CRC16	Response EOF
-	8 bits	8 bits	16 bits	-

Response parameter:

- Error code as Error_flag is set
  - 12h: the specified block is locked and its contents cannot be changed
  - 13h: the specified block was not successfully programmed

Figure 63. Write DSFID frame exchange between VCD and M24LR64E-R



When configured in the RF busy mode, the RF WIP/BUSY pin is tied to 0 from the SOF that starts the Write DSFID command to the end of the M24LR64E-R response.

When configured in the RF write in progress mode, the RF WIP/BUSY pin is tied to 0 for the duration of the internal write cycle (from the end of a valid Write DSFID command to the beginning of the M24LR64E-R response).

26.11 Lock DSFID

On receiving the Lock DSFID request, the M24LR64E-R locks the DSFID value permanently. The Option_flag is supported.

During the RF write cycle W_t, there should be no modulation (neither 100% nor 10%), otherwise the M24LR64E-R may not lock correctly the DSFID value in memory. The W_t time is equal to t_{1nom} + 18 × 302 µs.

Table 66. Lock DSFID request format

Request SOF	Request_flags	Lock DSFID	UID(1)	CRC16	Request EOF
-	8 bits	2Ah	64 bits	16 bits	-

1. Gray color means that the field is optional.

Request parameter:

- Request flags
- UID (optional)

Table 67. Lock DSFID response format when Error_flag is NOT set

Response SOF	Response_flags	CRC16	Response EOF
-	8 bits	16 bits	-

Response parameter:

- No parameter.

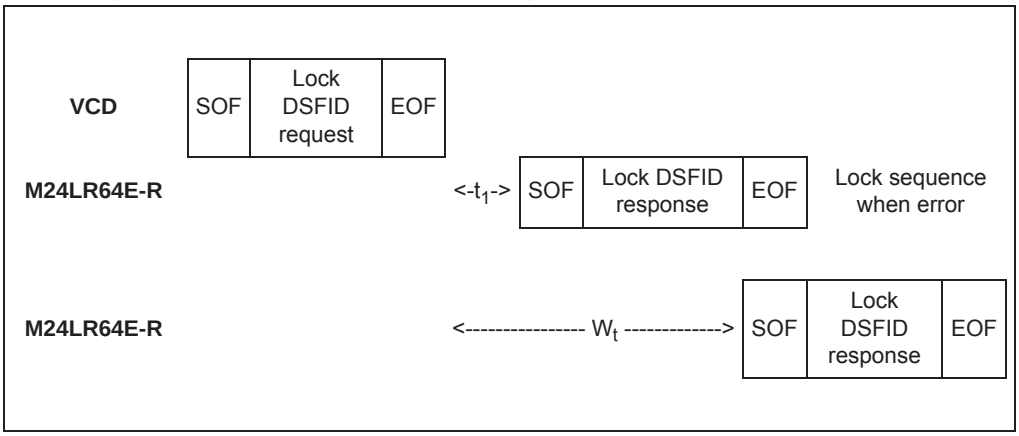
Table 68. Lock DSFID response format when Error_flag is set

Response SOF	Response_flags	Error code	CRC16	Response EOF
-	8 bits	8 bits	16 bits	-

Response parameter:

- Error code as Error_flag is set:
  - 11h: the specified block is already locked and thus cannot be locked again
  - 14h: the specified block was not successfully locked

Figure 64. Lock DSFID frame exchange between VCD and M24LR64E-R



When configured in the RF busy mode, the RF WIP/BUSY pin is tied to 0 from the SOF that starts the Lock DSFID command to the end of the M24LR64E-R response.

When configured in the RF write in progress mode, the RF WIP/BUSY pin is tied to 0 for the duration of the internal write cycle (from the end of a valid Lock DSFID command to the beginning of the M24LR64E-R response).

26.12 Get System Info

When receiving the Get System Info command, the M24LR64E-R sends back its information data in the response. The Option_flag is not supported. The Get System Info can be issued in both Addressed and Non Addressed modes.

The Protocol_extension_flag can be set to 0 or 1. *Table 70* and *Table 72* show M24LR64E-R response to the Get System Info command depending on the value of the Protocol_extension_flag.

Table 69. Get System Info request format

Request SOF	Request_flags	Get System Info	UID(1)	CRC16	Request EOF
-	8 bits	2Bh	64 bits	16 bits	-

1. Gray color means that the field is optional.

Request parameter:

- Request flags
- UID (optional)

Table 70. Get System Info response format when Protocol_extension_flag = 0 and Error_flag is NOT set

Response SOF	Response_ flags	Information flags	UID	DSFID	AFI	IC ref.	CRC16	Response EOF
-	00h	0Bh	64 bits	8 bits	8 bits	5Eh	16 bits	-

Response parameters:

- Information flags set to 0Ch. DSFID, AFI and IC reference fields are present.
- UID code on 64 bits
- DSFID value
- AFI value
- M24LR64E-R IC reference: the 8 bits are significant.

Table 71. Get System Info response format when Protocol_extension_flag = 1 and Error_flag is NOT set

Response SOF	Response _flags	Information flags	UID	DSFID	AFI	Memory size	IC ref	CRC16	Response EOF
-	00h	0Fh	64 bits	8 bits	8 bits	03 07FFh	5Eh	16 bits	-

Response parameters:

- Information flags set to 0Fh. DSFID, AFI, Memory Size and IC reference fields are present.
- UID code on 64 bits
- DSFID value
- AFI value
- Memory size. The M24LR64E-R provides 2048 blocks (07FFh) of 4 bytes (03h)
- IC reference: the 8 bits are significant.

Table 72. Get System Info response format when Error_flag is set

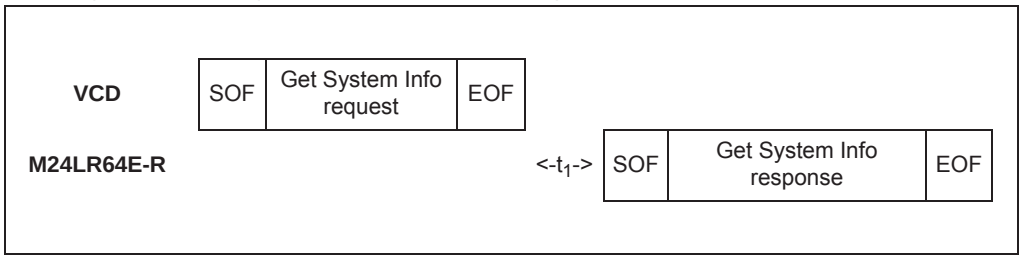
Response SOF	Response_flags	Error code	CRC16	Response EOF
-	01h	8 bits	16 bits	-

Response parameter:

- Error code as Error_flag is set:
  - 03h: Option not supported

.

Figure 65. Get System Info frame exchange between VCD and M24LR64E-R



When configured in the RF busy mode, the RF WIP/BUSY pin is tied to 0 from the SOF that starts the Get System Info command to the end of the M24LR64E-R response.

When configured in the RF write in progress mode, the RF WIP/BUSY pin remains in high-Z state.

26.13 Get Multiple Block Security Status

When receiving the Get Multiple Block Security Status command, the M24LR64E-R sends back the sector security status. The blocks are numbered from 00h to 01FFh in the request and the value is minus one (–1) in the field. For example, a value of '06' in the “Number of blocks” field requests to return the security status of seven blocks.

The Protocol_extension_flag should be set to 1 for the M24LR64E-R to operate correctly. If the Protocol_extension_flag is at 0, the M24LR64E-R answers with an error code.

During the M24LR64E-R response, if the internal block address counter reaches 01FFh, it rolls over to 0000h and the Sector Security Status bytes for that location are sent back to the reader.

Table 73. Get Multiple Block Security Status request format

Request SOF	Request _flags	Get Multiple Block Security Status	UID(1)	First block number	Number of blocks	CRC16	Request EOF
-	8 bits	2Ch	64 bits	16 bits	16 bits	16 bits	-

1. Gray color means that the field is optional.

Request parameter:

- Request flags
- UID (optional)
- First block number
- Number of blocks

Table 74. Get Multiple Block Security Status response format when Error_flag is NOT set

Response SOF	Response_flags	Sector security status	CRC16	Response EOF
-	8 bits	8 bits(1)	16 bits	-

1. Repeated as needed.

Response parameters:

- Sector security status (see *Table 75*)

Table 75. Sector security status

b_7	b_6	b_5	b_4	b_3	b_2	b_1	b_0
Reserved for future use All at 0			Password control bits		Read / Write protection bits		0: Current sector not locked 1: Current sector locked

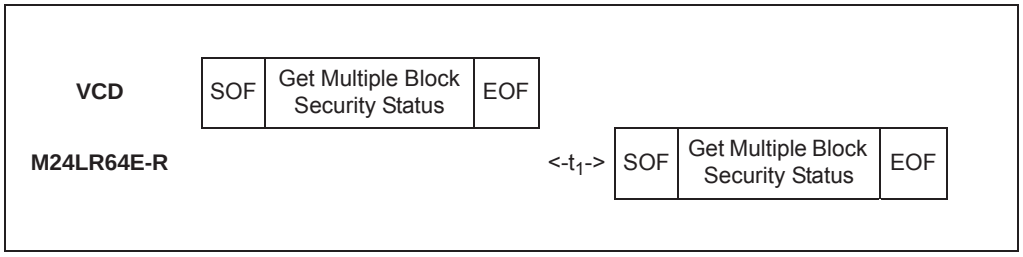
Table 76. Get Multiple Block Security Status response format when Error_flag is set

Response SOF	Response_flags	Error code	CRC16	Response EOF
-	8 bits	8 bits	16 bits	-

Response parameter:

- Error code as Error_flag is set:
  - 03h: the option is not supported
  - 10h: the specified block is not available

Figure 66. Get Multiple Block Security Status frame exchange between VCD and M24LR64E-R



When configured in the RF busy mode, the RF WIP/BUSY pin is tied to 0 from the SOF that starts the Get Multiple Block Security Status command to the end of the M24LR64E-R response.

When configured in the RF write in progress mode, the RF WIP/BUSY pin remains in high-Z state.

26.14 Write-sector Password

On receiving the Write-sector Password command, the M24LR64E-R uses the data contained in the request to write the password and reports whether the operation was successful in the response. The Option_flag is supported.

During the RF write cycle time, W_t, there must be no modulation at all (neither 100% nor 10%), otherwise the M24LR64E-R may not correctly program the data into the memory.

The W_t time is equal to t_{1nom} + 18 × 302 µs. After a successful write, the new value of the selected password is automatically activated. It is not required to present the new password value until M24LR64E-R power-down.

Table 77. Write-sector Password request format

Request SOF	Request _flags	Write-sector password	IC Mfg code	UID(1)	Password number	Data	CRC16	Request EOF
-	8 bits	B1h	02h	64 bits	8 bits	32 bits	16 bits	-

1. Gray color means that the field is optional.

Request parameter:

- Request flags
- UID (optional)
- Password number (01h = Pswd1, 02h = Pswd2, 03h = Pswd3, other = Error)
- Data

Table 78. Write-sector Password response format when Error_flag is NOT set

Response SOF	Response_flags	CRC16	Response EOF
-	8 bits	16 bits	-

Response parameter:

- no parameter.

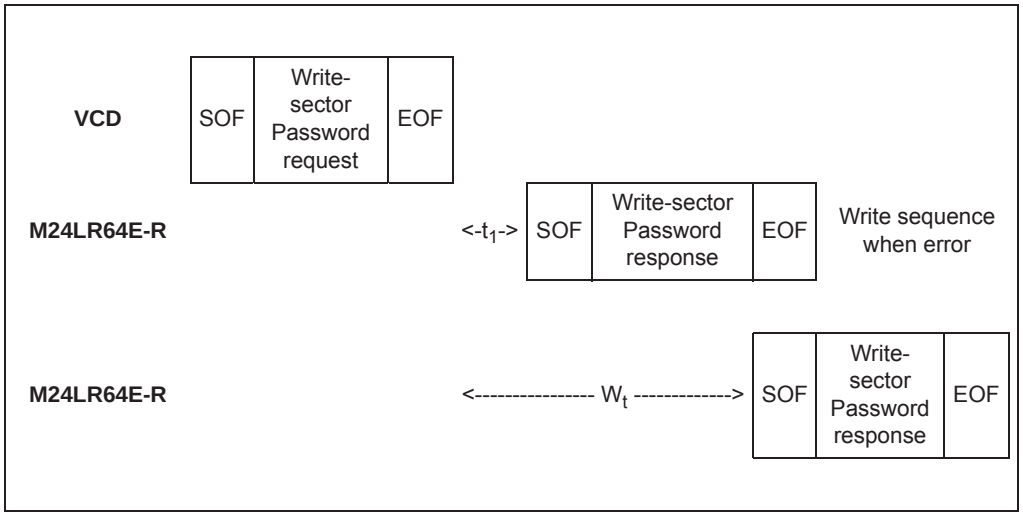
Table 79. Write-sector Password response format when Error_flag is set

Response SOF	Response_flags	Error code	CRC16	Response EOF
-	8 bits	8 bits	16 bits	-

Response parameter:

- Error code as Error_flag is set:
  - 10h: the password number is incorrect
  - 12h: the session was not opened before the password update
  - 13h: the specified block was not successfully programmed
  - 0Fh: the presented password is incorrect

Figure 67. Write-sector Password frame exchange between VCD and M24LR64E-R



When configured in the RF busy mode, the RF WIP/BUSY pin is tied to 0 from the SOF that starts the Write-sector Password command to the end of the M24LR64E-R response.

When configured in the RF write in progress mode, the RF WIP/BUSY pin is tied to 0 for the duration of the internal write cycle (from the end of a valid Write sector password command to the beginning of the M24LR64E-R response).

26.15 Lock-sector

On receiving the Lock-sector command, the M24LR64E-R sets the access rights and permanently locks the selected sector. The Option_flag is supported.

A sector is selected by giving the address of one of its blocks in the Lock-sector request (Sector number field). For example, addresses 0 to 31 are used to select sector 0 and addresses 32 to 63 are used to select sector 1. Care must be taken when issuing the Lock-sector command as all the blocks belonging to the same sector are automatically locked by a single command.

The Protocol_extension_flag should be set to 1 for the M24LR64E-R to operate correctly. If the Protocol_extension_flag is at 0, the M24LR64E-R answers with an error code.

During the RF write cycle W_t, there should be no modulation (neither 100% nor 10%), otherwise the M24LR64E-R may not correctly lock the memory block. The W_t time is equal to t_{1nom} + 18 × 302 µs.

Table 80. Lock-sector request format

Request SOF	Request _flags	Lock-sector	IC Mfg code	UID(1)	Sector number	Sector security status	CRC16	Request EOF
-	8 bits	B2h	02h	64 bits	16 bits	8 bits	16 bits	-

1. Gray color means that the field is optional.

Request parameters:

- Request flags
- (optional) UID
- Sector number
- Sector security status (refer to *Table 81*)

Table 81. Sector security status

b_7	b_6	b_5	b_4	b_3	b_2	b_1	b_0
0	0	0	Password control bits		Read / Write protection bits		1

Table 82. Lock-sector response format when Error_flag is NOT set

Response SOF	Response_flags	CRC16	Response EOF
-	8 bits	16 bits	-

Response parameter:

- No parameter

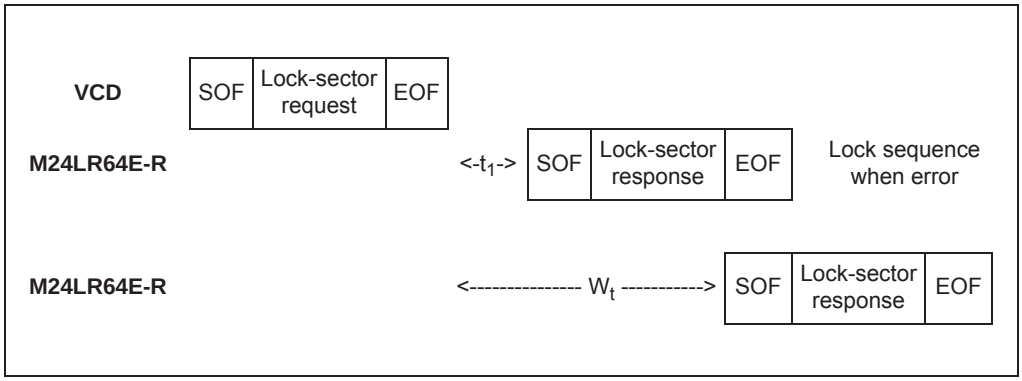
Table 83. Lock-sector response format when Error_flag is set

Response SOF	Response_flags	Error code	CRC16	Response EOF
-	8 bits	8 bits	16 bits	-

Response parameter:

- Error code as Error_flag is set:
  - 10h: the specified block is not available
  - 11h: the specified block is already locked and thus cannot be locked again
  - 14h: the specified block was not successfully locked

Figure 68. Lock-sector frame exchange between VCD and M24LR64E-R



When configured in the RF busy mode, the RF WIP/BUSY pin is tied to 0 from the SOF that starts the Lock-sector command to the end of the M24LR64E-R response.

When configured in the RF write in progress mode, the RF WIP/BUSY pin is tied to 0 for the duration of the internal write cycle (from the end of a valid Lock sector command to the beginning of the M24LR64E-R response).

26.16 Present-sector Password

On receiving the Present-sector Password command, the M24LR64E-R compares the requested password with the data contained in the request and reports whether the operation has been successful in the response. The Option_flag is supported.

During the comparison cycle equal to W_t, there should be no modulation (neither 100% nor 10%), otherwise the M24LR64E-R Password value may not be correctly compared. The W_t time is equal to t_{1nom} + 18 × 302 µs.

After a successful command, the access to all the memory blocks linked to the password is changed as described in *Section 4.1: M24LR64E-R block security in RF mode*.

Table 84. Present-sector Password request format

Request SOF	Request _flags	Present-sector Password	IC Mfg code	UID(1)	Password number	Password	CRC16	Request EOF
-	8 bits	B3h	02h	64 bits	8 bits	32 bits	16 bits	-

1. Gray color means that the field is optional.

Request parameter:

- Request flags
- UID (optional)
- Password Number (0x01 = Pswd1, 0x02 = Pswd2, 0x03 = Pswd3, other = Error)
- Password

Table 85. Present-sector Password response format when Error_flag is NOT set

Response SOF	Response_flags	CRC16	Response EOF
-	8 bits	16 bits	-

Response parameter:

- No parameter. The response is sent back after the write cycle.

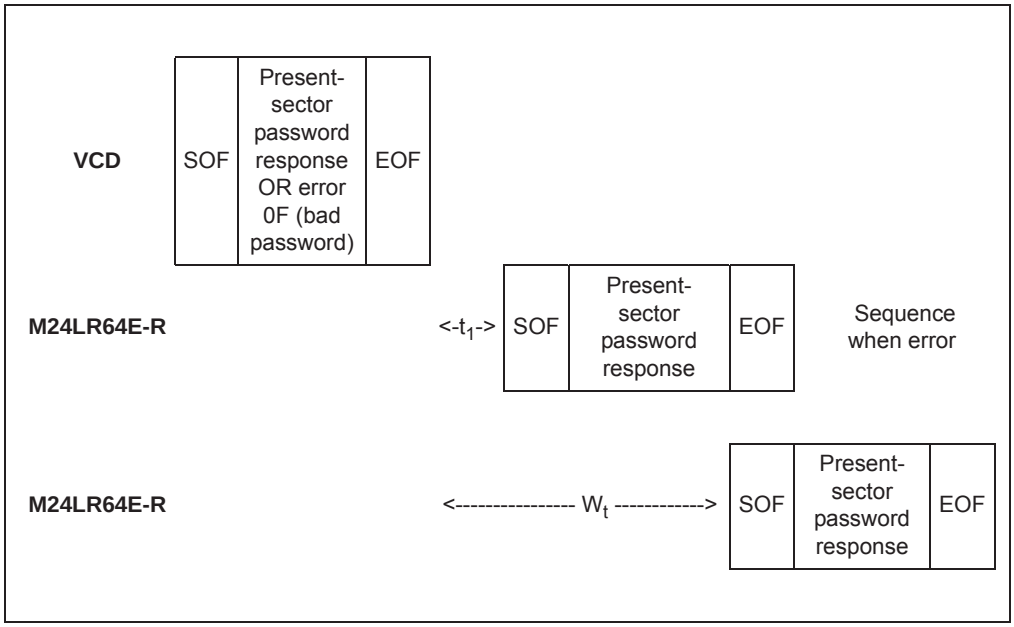
Table 86. Present-sector Password response format when Error_flag is set

Response SOF	Response_flags	Error code	CRC16	Response EOF
-	8 bits	8 bits	16 bits	-

Response parameter:

- Error code as Error_flag is set:
  - 10h: the password number is incorrect
  - 0Fh: the present password is incorrect

Figure 69. Present-sector Password frame exchange between VCD and M24LR64E-R



When configured in the RF busy mode, the RF WIP/BUSY pin is tied to 0 from the SOF that starts the Present Sector Password command to the end of the M24LR64E-R response.

When configured in the RF write in progress mode, the RF WIP/BUSY remains in high-Z state.

26.17 Fast Read Single Block

On receiving the Fast Read Single Block command, the M24LR64E-R reads the requested block and sends back its 32-bit value in the response. The Option_flag is supported. The data rate of the response is multiplied by 2.

The Protocol_extension_flag should be set to 1 for the M24LR64E-R to operate correctly. If the Protocol_extension_flag is at 0, the M24LR64E-R answers with an error code.

The subcarrier_flag should be set to 0, otherwise the M24LR64E-R answers with an error code.

Table 87. Fast Read Single Block request format

Request SOF	Request_flags	Fast Read Single Block	IC Mfg code	UID(1)	Block number	CRC16	Request EOF
-	8 bits	C0h	02h	64 bits	16 bits	16 bits	-

1. Gray color means that the field is optional.

Request parameters:

- Request flags
- UID (optional)
- Block number

Table 88. Fast Read Single Block response format when Error_flag is NOT set

Response SOF	Response_flags	Sector security status(1)	Data	CRC16	Response EOF
-	8 bits	8 bits	32 bits	16 bits	-

1. Gray color means that the field is optional.

Response parameters:

- Sector security status if Option_flag is set (see *Table 89*)
- Four bytes of block data

Table 89. Sector security status

b_7	b_6	b_5	b_4	b_3	b_2	b_1	b_0
Reserved for future use All at 0			Password control bits		Read / Write protection bits		0: Current sector not locked 1: Current sector locked

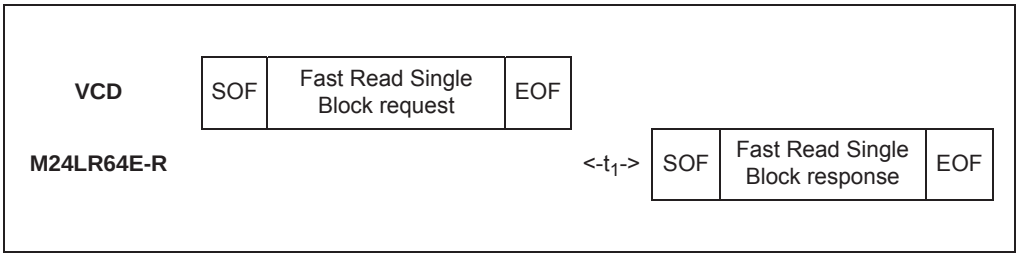
Table 90. Fast Read Single Block response format when Error_flag is set

Response SOF	Response_flags	Error code	CRC16	Response EOF
-	8 bits	8 bits	16 bits	-

Response parameter:

- Error code as Error_flag is set:
  - 10h: the specified block is not available
  - 15h: the specified block is read-protected

Figure 70. Fast Read Single Block frame exchange between VCD and M24LR64E-R



When configured in the RF busy mode, the RF WIP/BUSY pin is tied to 0 from the SOF that starts the Fast Read Single block command to the end of the M24LR64E-R response.

When configured in the RF write in progress mode, the RF WIP/BUSY pin remains in high-Z state.

26.18 Fast Inventory Initiated

Before receiving the Fast Inventory Initiated command, the M24LR64E-R must have received an Initiate or a Fast Initiate command in order to set the Initiate_ flag. If not, the M24LR64E-R does not answer the Fast Inventory Initiated command.

The subcarrier_flag should be set to 0, otherwise the M24LR64E-R answers with an error code.

On receiving the Fast Inventory Initiated request, the M24LR64E-R runs the anticollision sequence. The Inventory_flag must be set to 1. The meaning of flags 5 to 8 is shown in *Table 29*. The data rate of the response is multiplied by 2.

The request contains:

- the flags,
- the Inventory command code,
- the AFI if the AFI flag is set,
- the mask length,
- the mask value,
- the CRC.

The M24LR64E-R does not generate any answer in case of error.

Table 91. Fast Inventory Initiated request format

Request SOF	Request _flags	Fast Inventory Initiated	IC Mfg code	Optional AFI	Mask length	Mask value	CRC16	Request EOF
-	8 bits	C1h	02h	8 bits	8 bits	0 - 64 bits	16 bits	-

The Response contains:

- the flags,
- the Unique ID.

Table 92. Fast Inventory Initiated response format

Response SOF	Response_flags	DSFID	UID	CRC16	Response EOF
-	8 bits	8 bits	64 bits	16 bits	-

During an Inventory process, if the VCD does not receive an RF M24LR64E-R response, it waits for a time t_3 before sending an EOF to switch to the next slot. t_3 starts from the rising edge of the request EOF sent by the VCD.

- If the VCD sends a 100% modulated EOF, the minimum value of t_3 is:
  $t_3 min = 4384/f_C$ (323.3µs) + t_{SOF}
- If the VCD sends a 10% modulated EOF, the minimum value of t_3 is:
  $t_3 min = 4384/f_C$ (323.3µs) + t_{NRT}

where:

- t_{SOF} is the time required by the M24LR64E-R to transmit an SOF to the VCD
- t_{NRT} is the nominal response time of the M24LR64E-R

t_{NRT} and t_{SOF} are dependent on the M24LR64E-R-to-VCD data rate and subcarrier modulation mode.

When configured in the RF busy mode, the RF WIP/BUSY pin is driven to 0 from the SOF starting the inventory command to the end of the M24LR64E-R response. If the M24LR64E-R does not receive the corresponding slot marker, the RF WIP/BUSY pin remains at 0 until the next RF power-off.

When configured in the RF write in progress mode, the RF WIP/BUSY pin remains in high-Z state.

26.19 Fast Initiate

On receiving the Fast Initiate command, the M24LR64E-R sets the internal Initiate_flag and sends back a response only if it is in the Ready state. The command has to be issued in the Non Addressed mode only (Select_flag is reset to 0 and Address_flag is reset to 0). If an error occurs, the M24LR64E-R does not generate any answer. The Initiate_flag is reset after a power-off of the M24LR64E-R. The data rate of the response is multiplied by 2.

The subcarrier_flag should be set to 0, otherwise the M24LR64E-R answers with an error code.

The request contains:

- No data

Table 93. Fast Initiate request format

Request SOF	Request_flags	Fast Initiate	IC Mfg Code	CRC16	Request EOF
-	8 bits	C2h	02h	16 bits	-

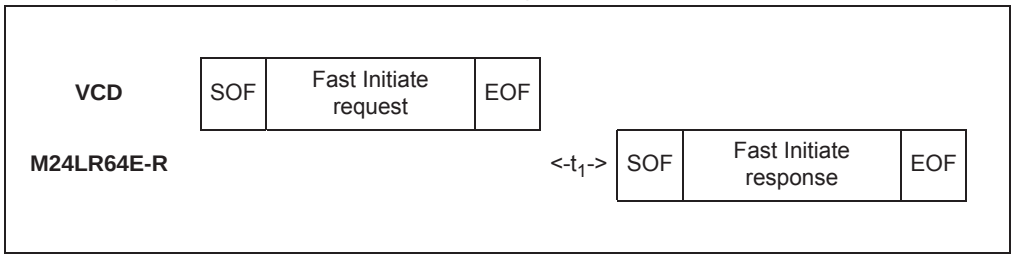
The response contains:

- the flags,
- the Unique ID.

Table 94. Fast Initiate response format

Response SOF	Response_flags	DSFID	UID	CRC16	Response EOF
-	8 bits	8 bits	64 bits	16 bits	-

Figure 71. Fast Initiate frame exchange between VCD and M24LR64E-R



When configured in the RF busy mode, the RF WIP/BUSY pin is tied to 0 from the SOF that starts the Fast Initiate command to the end of the M24LR64E-R response.

When configured in the RF write in progress mode, the RF WIP/BUSY pin remains in high-Z state.

26.20 Fast Read Multiple Block

On receiving the Fast Read Multiple Block command, the M24LR64E-R reads the selected blocks and sends back their value in multiples of 32 bits in the response. The blocks are numbered from 00h to 1FFh in the request and the value is minus one (–1) in the field. For example, if the “Number of blocks” field contains the value 06h, seven blocks are read. The maximum number of blocks is fixed to 32 assuming that they are all located in the same sector. If the number of blocks overlaps sectors, the M24LR64E-R returns an error code.

The Protocol_extension_flag should be set to 1 for the M24LR64E-R to operate correctly. If the Protocol_extension_flag is at 0, the M24LR64E-R answers with an error code.

The Option_flag is supported. The data rate of the response is multiplied by 2.

The subcarrier_flag should be set to 0, otherwise the M24LR64E-R answers with an error code.

Table 95. Fast Read Multiple Block request format

Request SOF	Request_ flags	Fast Read Multiple Block	IC Mfg code	UID(1)	First block number	Number of blocks	CRC16	Request EOF
-	8 bits	C3h	02h	64 bits	16 bits	8 bits	16 bits	-

1. Gray color means that the field is optional.

Request parameters:

- Request flag
- UID (Optional)
- First block number
- Number of blocks

Table 96. Fast Read Multiple Block response format when Error_flag is NOT set

Response SOF	Response_flags	Sector security status(1)	Data	CRC16	Response EOF
-	8 bits	8 bits(2)	32 bits(2)	16 bits	-

1. Gray color means that the field is optional.
2. Repeated as needed.

Response parameters:

- Sector security status if Option_flag is set (see *Table 97*)
- N block of data

Table 97. Sector security status if Option_flag is set

b_7	b_6	b_5	b_4	b_3	b_2	b_1	b_0
Reserved for future use All at 0			Password control bits		Read / Write protection bits		0: Current sector not locked 1: Current sector locked

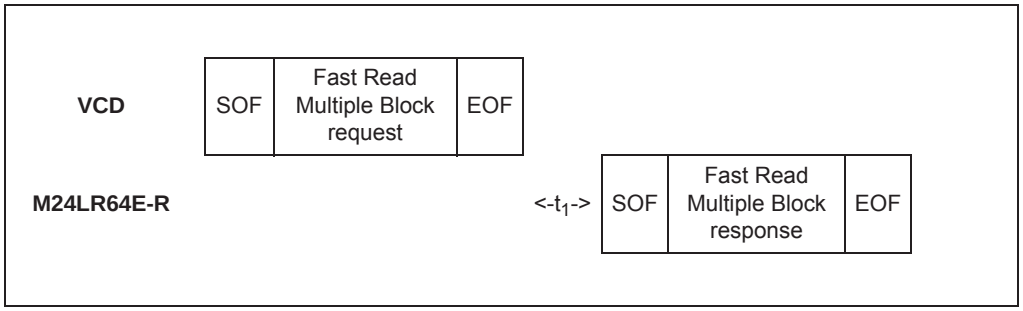
Table 98. Fast Read Multiple Block response format when Error_flag is set

Response SOF	Response_flags	Error code	CRC16	Response EOF
-	8 bits	8 bits	16 bits	-

Response parameter:

- Error code as Error_flag is set:
  - 03h: the option is not supported
  - 10h: block address not available
  - 15h: block read-protected

Figure 72. Fast Read Multiple Block frame exchange between VCD and M24LR64E-R



When configured in the RF busy mode, the RF WIP/BUSY pin is tied to 0 from the SOF that starts the Fast Read Multiple Block command to the end of the M24LR64E-R response.

When configured in the RF write in progress mode, the RF WIP/BUSY pin remains in high-Z state.

26.21 Inventory Initiated

Before receiving the Inventory Initiated command, the M24LR64E-R must have received an Initiate or a Fast Initiate command in order to set the Initiate_ flag. If not, the M24LR64E-R does not answer the Inventory Initiated command.

On receiving the Inventory Initiated request, the M24LR64E-R runs the anticollision sequence. The Inventory_flag must be set to 1. The meaning of flags 5 to 8 is given in *Table 29 on page 68*.

The request contains:

- the flags,
- the Inventory Command code,
- the AFI if the AFI flag is set,
- the mask length,
- the mask value,
- the CRC.

The M24LR64E-R does not generate any answer in case of error.

Table 99. Inventory Initiated request format

Request SOF	Request _flags	Inventory Initiated	IC Mfg code	Optional AFI	Mask length	Mask value	CRC16	Request EOF
-	8 bits	D1h	02h	8 bits	8 bits	0 - 64 bits	16 bits	-

The response contains:

- the flags,
- the Unique ID.

Table 100. Inventory Initiated response format

Response SOF	Response_flags	DSFID	UID	CRC16	Response EOF
-	8 bits	8 bits	64 bits	16 bits	-

During an Inventory process, if the VCD does not receive an RF M24LR64E-R response, it waits for a time t_3 before sending an EOF to switch to the next slot. t_3 starts from the rising edge of the request EOF sent by the VCD.

- If the VCD sends a 100% modulated EOF, the minimum value of t_3 is:
  $t_3 min = 4384/f_C$ (323.3µs) + t_{SOF}
- If the VCD sends a 10% modulated EOF, the minimum value of t_3 is:
  $t_3 min = 4384/f_C$ (323.3µs) + t_{NRT}

where:

- t_{SOF} is the time required by the M24LR64E-R to transmit an SOF to the VCD
- t_{NRT} is the nominal response time of the M24LR64E-R

t_{NRT} and t_{SOF} are dependent on the M24LR64E-R-to-VCD data rate and subcarrier modulation mode.

When configured in the RF busy mode, the RF WIP/BUSY pin is tied to 0 from the SOF starting the inventory command to the end of the M24LR64E-R response. If the M24LR64E-R does not receive the corresponding slot marker, the RF WIP/BUSY pin remains at 0 until the next RF power-off.

When configured in the RF write in progress mode, the RF WIP/BUSY pin remains in high-Z state.

26.22 Initiate

On receiving the Initiate command, the M24LR64E-R sets the internal Initiate_flag and sends back a response only if it is in the ready state. The command has to be issued in the Non Addressed mode only (Select_flag is reset to 0 and Address_flag is reset to 0). If an error occurs, the M24LR64E-R does not generate any answer. The Initiate_flag is reset after a power-off of the M24LR64E-R.

The request contains:

- No data

Table 101. Initiate request format

Request SOF	Request_flags	Initiate	IC Mfg code	CRC16	Request EOF
-	8 bits	D2h	02h	16 bits	-

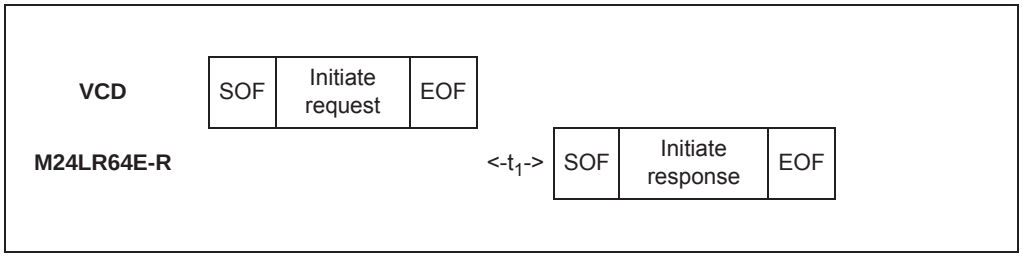
The response contains:

- the flags,
- the Unique ID.

Table 102. Initiate response format

Response SOF	Response_flags	DSFID	UID	CRC16	Response EOF
-	8 bits	8 bits	64 bits	16 bits	-

Figure 73. Initiate frame exchange between VCD and M24LR64E-R



When configured in the RF busy mode, the RF WIP/BUSY pin is tied to 0 from the SOF that starts the Initiate command to the end of the M24LR64E-R response.

When configured in the RF write in progress mode, the RF WIP/BUSY pin remains in high-Z state.

26.23 ReadCfg

On receiving the ReadCfg command, the M24LR64E-R reads the Configuration byte and sends back its 8-bit value in the response.

The Protocol_extension_flag should be set to 0 for the M24LR64E-R to operate correctly. If the Protocol_extension_flag is at 1, the M24LR64E-R answers with an error code. The Option_flag is not supported. The Inventory_flag must be set to 0.

Table 103. ReadCfg request format

Request SOF	Request_flags	ReadCfg	IC Mfg code	UID(1)	CRC16	Request EOF
-	8 bits	A0h	02h	64 bits	16 bits	-

1. Gray color means that the field is optional.

Request parameters:

- UID (optional)

Table 104. ReadCfg response format when Error_flag is NOT set

Response SOF	Response_flags	Data	CRC16	Response EOF
-	8 bits	8 bits	16 bits	-

Response parameters:

- One byte of data: Configuration byte

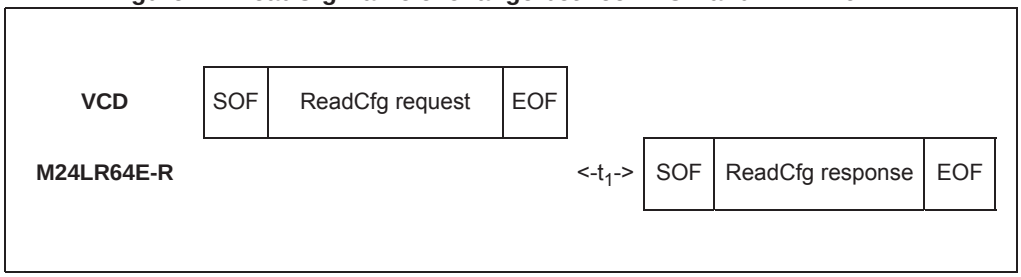
Table 105. ReadCfg response format when Error_flag is set

Response SOF	Response_flags	Error code	CRC16	Response EOF
-	8 bits	8 bits	16 bits	-

Response parameter:

- Error code as Error_flag is set
  - 03h: the option is not supported
  - 0Fh: error with no information given

Figure 74. ReadCfg frame exchange between VCD and M24LR64E-R



When configured in the RF busy mode, the RF WIP/BUSY pin is tied to 0 from the SOF that starts the ReadCfg command to the end of the M24LR64E-R response.

When configured in the RF write in progress mode, the RF WIP/BUSY pin remains in high-Z state.

26.24 WriteEHCfg

On receiving the WriteEHCfg command, the M24LR64E-R writes the data contained in the request to the Configuration byte and reports whether the write operation was successful in the response. The Protocol_extension_flag should be set to 0 for the M24LR64E-R to operate correctly. If the Protocol_extension_flag is at 1, the M24LR64E-R answers with an error code.

The Option_flag is supported, the Inventory_flag is not supported.

During the RF write cycle W_t, there should be no modulation (neither 100% nor 10%), otherwise the M24LR64E-R may not program correctly the data into the Configuration byte. The W_t time is equal to t_{1nom} + 18 × 302 µs.

Table 106. WriteEHCfg request format

Request SOF	Request_flags	WriteEHCfg	IC Mfg code	UID(1)	Data	CRC16	Request EOF
-	8 bits	A1h	02h	64 bits	8 bits	16 bits	-

1. Gray color means that the field is optional.

Request parameters:

- Request flags
- UID (optional)
- Data: during WriteEHCfg command, bit 3 of the data is ignored (see *Table 14*).

Table 107. WriteEHCfg response format when Error_flag is NOT set

Response SOF	Response_flags	CRC16	Response EOF
-	8 bits	16 bits	-

Response parameter:

- No parameter. The response is sent back after the writing cycle.

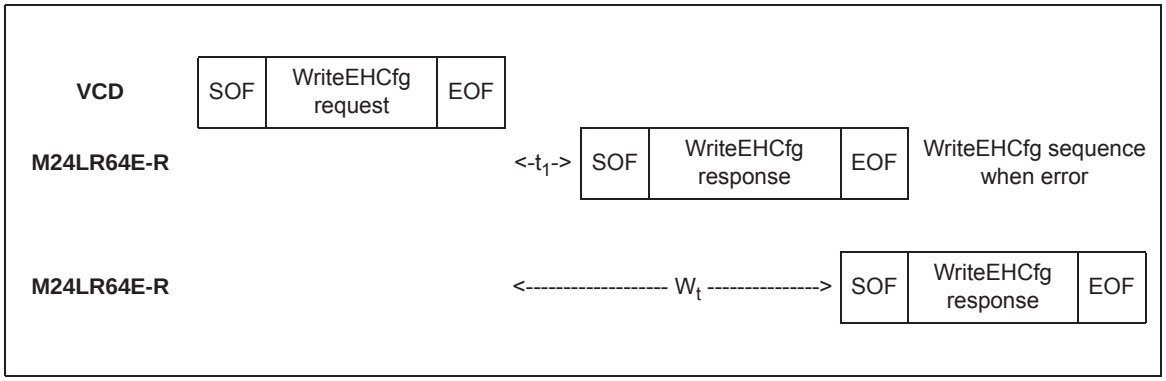
Table 108. WriteEHCfg response format when Error_flag is set

Response SOF	Response_flags	Error code	CRC16	Response EOF
-	8 bits	8 bits	16 bits	-

Response parameter:

- Error code as Error_flag is set:
  - 13h: the specified block was not successfully programmed

Figure 75. WriteEHCfg frame exchange between VCD and M24LR64E-R



When configured in the RF busy mode, the RF WIP/BUSY pin is tied to 0 from the SOF that starts the WriteEHCfg command to the end of the M24LR64E-R response.

When configured in the RF write in progress mode, the RF WIP/BUSY pin is tied to 0 for the entire duration of the internal write cycle (from the end of a valid WriteEHCfg command to the beginning of the M24LR64E-R response).

26.25 WriteDOCfg

On receiving the WriteDOCfg command, the M24LR64E-R writes the data contained in the request to the Configuration byte and reports whether the write operation was successful in the response. The Protocol_extension_flag should be set to 0 for the M24LR64E-R to operate correctly. If the Protocol_extension_flag is at 1, the M24LR64E-R answers with an error code.

The Option_flag is supported, the Inventory_flag is not supported.

During the RF write cycle W_t, there should be no modulation (neither 100% nor 10%), otherwise the M24LR64E-R may not program correctly the data into the Configuration byte. The W_t time is equal to t_{1nom} + 18 × 302 µs.

Table 109. WriteDOCfg request format

Request SOF	Request_ flags	WriteDOCfg	IC Mfg code	UID(1)	Data	CRC16	Request EOF
-	8 bits	A4h	02h	64 bits	8 bits	16 bits	-

1. Gray color means that the field is optional.

Request parameters:

- Request flag
- UID (optional)
- Data: during a WriteDOCfg command, bits 2 to 0 of the data are ignored (see *Table 14*).

Table 110. WriteDOCfg response format when Error_flag is NOT set

Response SOF	Response_flags	CRC16	Response EOF
-	8 bits	16 bits	-

Response parameter:

- No parameter. The response is sent back after the writing cycle.

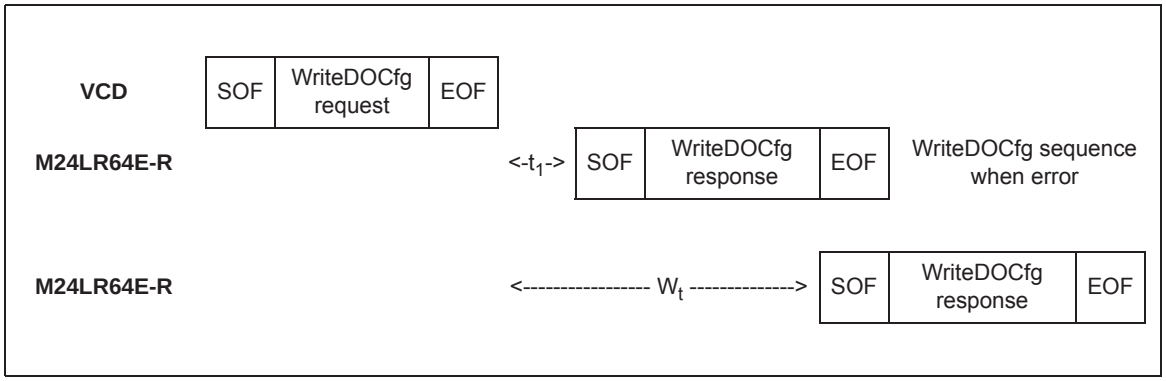
Table 111. WriteDOCfg response format when Error_flag is set

Response SOF	Response_flags	Error code	CRC16	Response EOF
-	8 bits	8 bits	16 bits	-

Response parameter:

- Error code as Error_flag is set:
  - 13h: the specified block was not successfully programmed

Figure 76. WriteDOCfg frame exchange between VCD and M24LR64E-R



When configured in the RF busy mode, the RF WIP/BUSY pin is tied to 0 from the SOF that starts the WriteEHCfg command to the end of the M24LR64E-R response.

When configured in the RF write in progress mode, the RF WIP/BUSY pin is tied to 0 for the entire duration of the internal write cycle (from the end of a valid WriteDOCfg command to the beginning of the M24LR64E-R response).

26.26 SetRstEHEn

On receiving the SetRstEHEn command, the M24LR64E-R sets or resets the EH_enable bit in the volatile Control register. The Protocol_extension_flag should be set to 0 for the M24LR64E-R to operate correctly. If the Protocol_extension_flag is at 1, the M24LR64E-R answers with an error code. The Option_flag and the Inventory_flag are not supported.

Table 112. SetRstEHEn request format

Request SOF	Request_flags	SetRstEHEn	IC Mfg code	UID(1)	Data	CRC16	Request EOF
-	8 bits	A2h	02h	64 bits	8 bits	16 bits	-

1. Gray color means that the field is optional.

Request parameters:

- Request flags
- UID (optional)
- Data: during a SetRstEHEn command, bits 7 to 1 are ignored. Bit 0 is the EH_enable bit.

Table 113. SetRstEHEn response format when Error_flag is NOT set

Response SOF	Response_flags	CRC16	Response EOF
-	8 bits	16 bits	-

Response parameter:

- No parameter. The response is sent back after t_1.

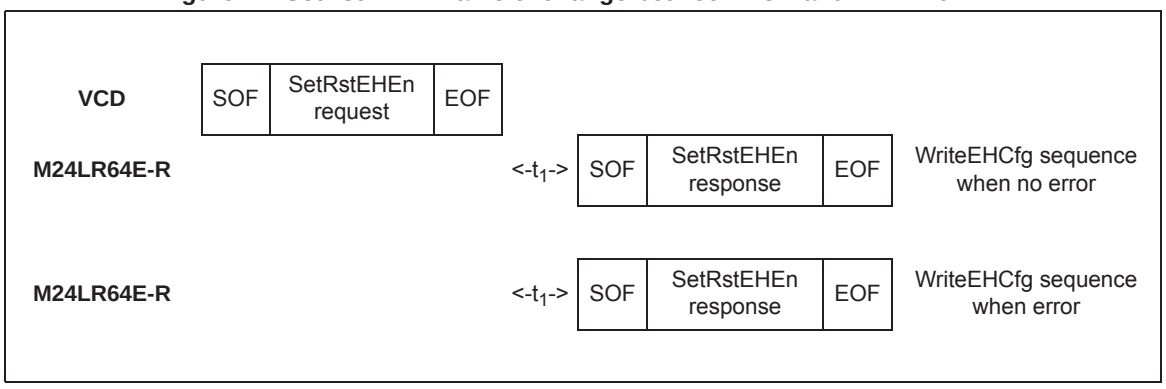
Table 114. SetRstEHEn response format when Error_flag is set

Response SOF	Response_flags	Error code	CRC16	Response EOF
-	8 bits	8 bits	16 bits	-

Response parameter:

- Error code as Error_flag is set:
  - 03h: the option is not supported

Figure 77. SetRstEHEn frame exchange between VCD and M24LR64E-R



When configured in the RF busy mode, the RF WIP/BUSY pin is tied to 0 from the SOF that starts the SetRstEHEn command to the end of the M24LR64E-R response.

When configured in the RF write in progress mode, the RF WIP/BUSY pin remains in high-Z state.

26.27 CheckEHEn

On receiving the CheckEHEn command, the M24LR64E-R reads the Control register and sends back its 8-bit value in the response.

The Protocol_extension_flag should be set to 0 for the M24LR64E-R to operate correctly. If the Protocol_extension_flag is at 1, the M24LR64E-R answers with an error code. The Option_flag is not supported. The Inventory_flag must be set to 0.

Table 115. CheckEHEn request format

Request SOF	Request_flags	CheckEHEn	IC Mfg code	UID(1)	CRC16	Request EOF
-	8 bits	A3h	02h	64 bits	16 bits	-

1. Gray color means that the field is optional.

Request parameters:

- UID (optional)

Table 116. CheckEHEn response format when Error_flag is NOT set

Response SOF	Response_flags	Data	CRC16	Response EOF
-	8 bits	8 bits	16 bits	-

Response parameters:

- One byte of data: volatile Control register (see *Table 15*)

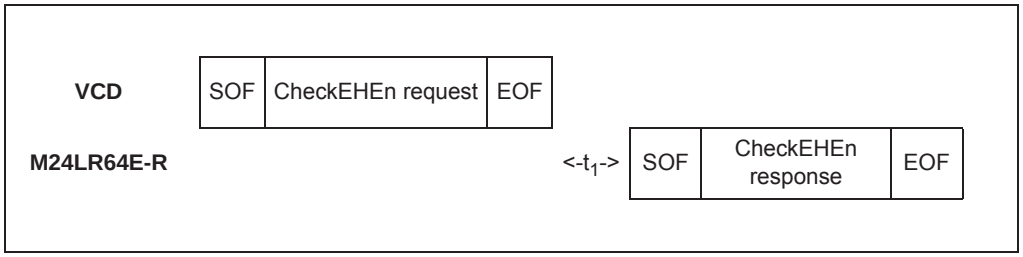
Table 117. CheckEHEn response format when Error_flag is set

Response SOF	Response_flags	Error code	CRC16	Response EOF
-	8 bits	8 bits	16 bits	-

Response parameter:

- Error code as Error_flag is set
  - 03h: the option is not supported

Figure 78. CheckEHEn frame exchange between VCD and M24LR64E-R



When configured in the RF busy mode, the RF WIP/BUSY pin is tied to 0 from the SOF that starts the CheckEHEn command to the end of the M24LR64E-R response.

When configured in the RF write in progress mode, the RF WIP/BUSY pin remains in high-Z state.

27 Maximum ratings

Stressing the device above the rating listed in *Table 118* may cause permanent damage to the device. These are stress ratings only and operation of the device, at these or any other conditions above those indicated in the operating sections of this specification, is not implied. Exposure to absolute maximum rating conditions for extended periods may affect the device reliability. Refer also to the STMicroelectronics SURE Program and other relevant quality documents.

Table 118. Absolute maximum ratings

Symbol	Parameter		Min.	Max.	Unit
T_A	Ambient operating temperature		-40	85	°C
T_{STG}, h_{STG}, t_{STG}	Storage conditions	Sawn wafer on UV tape	15	25	°C
			-	9(1)	months
			Kept in its original packing form		
T_{STG}	Storage temperature	UFDFPN8 (MLP8), SO8, TSSOP8	-65	150	°C
T_{LEAD}	Lead temperature during soldering	UFDFPN8 (MLP8), SO8, TSSOP8	See note (2)		°C
V_{IO}	I^2C input or output range		-0.50	6.5	V
V_{CC}	I^2C supply voltage		-0.50	6.5	V
I_{OL_MAX}	DC output current on pin SDA or RF WIP/BUSY (when equal to 0)		-	5	mA
I_{CC}(3)	RF supply current AC0 - AC1		-	50	mA
V_{MAX_1}(3)	RF input voltage amplitude peak to peak between AC0 and AC1, GND pad left floating	VAC0-VAC1	-	27	V
V_{MAX_2}(3)	AC voltage between AC0 and GND, or AC1 and GND	VAC0-GND, or VAC1-GND	-1	11	V
V_{ESD}	Electrostatic discharge voltage (human body model)(4)	AC0, AC1	-	1000	V
		Other pads	-	3500	
	Electrostatic discharge voltage on antenna (5)	AC0, AC1	-	4000	

1. Counted from ST shipment date.
2. Compliant with JEDEC Std J-STD-020C (for small body, Sn-Pb or Pb assembly), the ST ECOPACK® 7191395 specification, and the European directive on Restrictions on Hazardous Substances (RoHS) 2002/95/EU.
3. Based on characterization, not tested in production.
4. AEC-Q100-002 (compliant with JEDEC Std JESD22-A114, C1 = 100 pF, R1 = 1500 Ω, R2 = 500 Ω)
5. Compliant with IEC 61000-4-3 method. (M24LRxxE packaged in S08N is mounted on ST's reference antenna ANT1- M24LRxxE)

28 I²C DC and AC parameters

This section summarizes the operating and measurement conditions, and the DC and AC characteristics of the device in I²C mode. The parameters in the DC and AC characteristic tables that follow are derived from tests performed under the measurement conditions summarized in the relevant tables. Designers should check that the operating conditions in their circuit match the measurement conditions when relying on the quoted parameters.

Table 119. I²C operating conditions

Symbol	Parameter	Min.	Max.	Unit
V_{CC}	Supply voltage	1.8	5.5	V
T_A	Ambient operating temperature	-40	85	°C

Table 120. AC test measurement conditions

Symbol	Parameter	Min.	Max.	Unit
C_L	Load capacitance	100		pF
t_r, t_f	Input rise and fall times	-	50	ns
V_{hi-lo}	Input levels	0.2 V_{CC} to 0.8 V_{CC}		V
$V_{ref(t)}$	Input and output timing reference levels	0.3 V_{CC} to 0.7 V_{CC}		V

Figure 79. AC test measurement I/O waveform

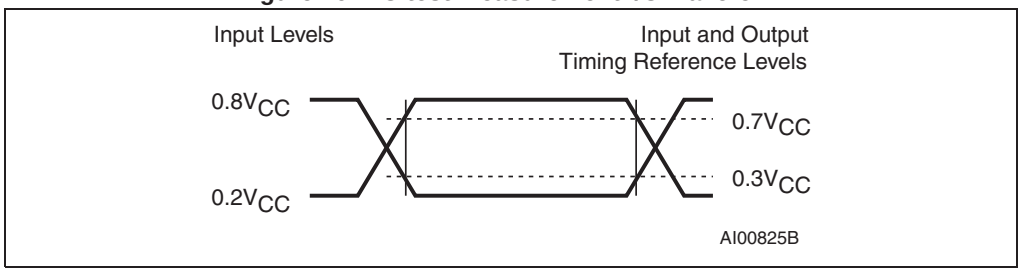


Table 121. Input parameters

Symbol	Parameter	Min.	Max.	Unit
C_{IN}	Input capacitance (SDA)	-	8	pF
C_{IN}	Input capacitance (other pins)	-	6	pF
t_{NS}(1)	Pulse width ignored (Input filter on SCL and SDA)	-	80	ns

1. Characterized only.

Table 122. I²C DC characteristics

Symbol	Parameter	Test condition	Min.	Max.	Unit
I_{LI}	Input leakage current (SCL, SDA)	$V_{IN} = V_{SS}$ or V_{CC} device in Standby mode	-	± 2	µA
I_{LO_Vout}	V_{out} output leakage current	External voltage applied on V_{out}: V_{SS} or V_{CC}	-	± 5	µA
I_{LO}	Output leakage current	SDA in Hi-Z, external voltage applied on SDA: V_{SS} or V_{CC}	-	± 2	µA
I_{CC}	Supply current (Read)(1)	V_{CC} = 1.8 V, f_c = 100 kHz (rise/fall time < 50 ns)	-	50	µA
		V_{CC} = 1.8 V, f_c = 400 kHz (rise/fall time < 50 ns)	-	100	
		V_{CC} = 2.5 V, f_c = 400 kHz (rise/fall time < 50 ns)	-	200	
		V_{CC} = 5.5 V, f_c = 400 kHz (rise/fall time < 50 ns)	-	400	
I_{CC0}	Supply current (Write)(1)	V_{CC} = 1.8 - 5.5 V	-	220	µA
I_{CC1}	Standby supply current	$V_{IN} = V_{SS}$ or V_{CC} V_{CC} = 1.8 V	-	30	µA
		$V_{IN} = V_{SS}$ or V_{CC} V_{CC} = 2.5 V	-	30	
		$V_{IN} = V_{SS}$ or V_{CC} V_{CC} = 5.5 V	-	100	
V_{IL}	Input low voltage (SDA, SCL)	V_{CC} = 1.8 V	-0.45	$0.25V_{CC}$	V
		V_{CC} = 2.5 V	-0.45	$0.25V_{CC}$	
		V_{CC} = 5.5 V	-0.45	$0.3V_{CC}$	
V_{IH}	Input high voltage (SDA, SCL)	V_{CC} = 1.8 V	$0.75V_{CC}$	V_{CC}+1	V
		V_{CC} = 2.5 V	$0.75V_{CC}$	V_{CC}+1	
		V_{CC} = 5.5 V	$0.7V_{CC}$	V_{CC}+1	
V_{OL}	Output low voltage	I_{OL} = 2.1 mA, V_{CC} = 1.8 V or I_{OL} = 3 mA, V_{CC} = 5.5 V	-	0.4	V

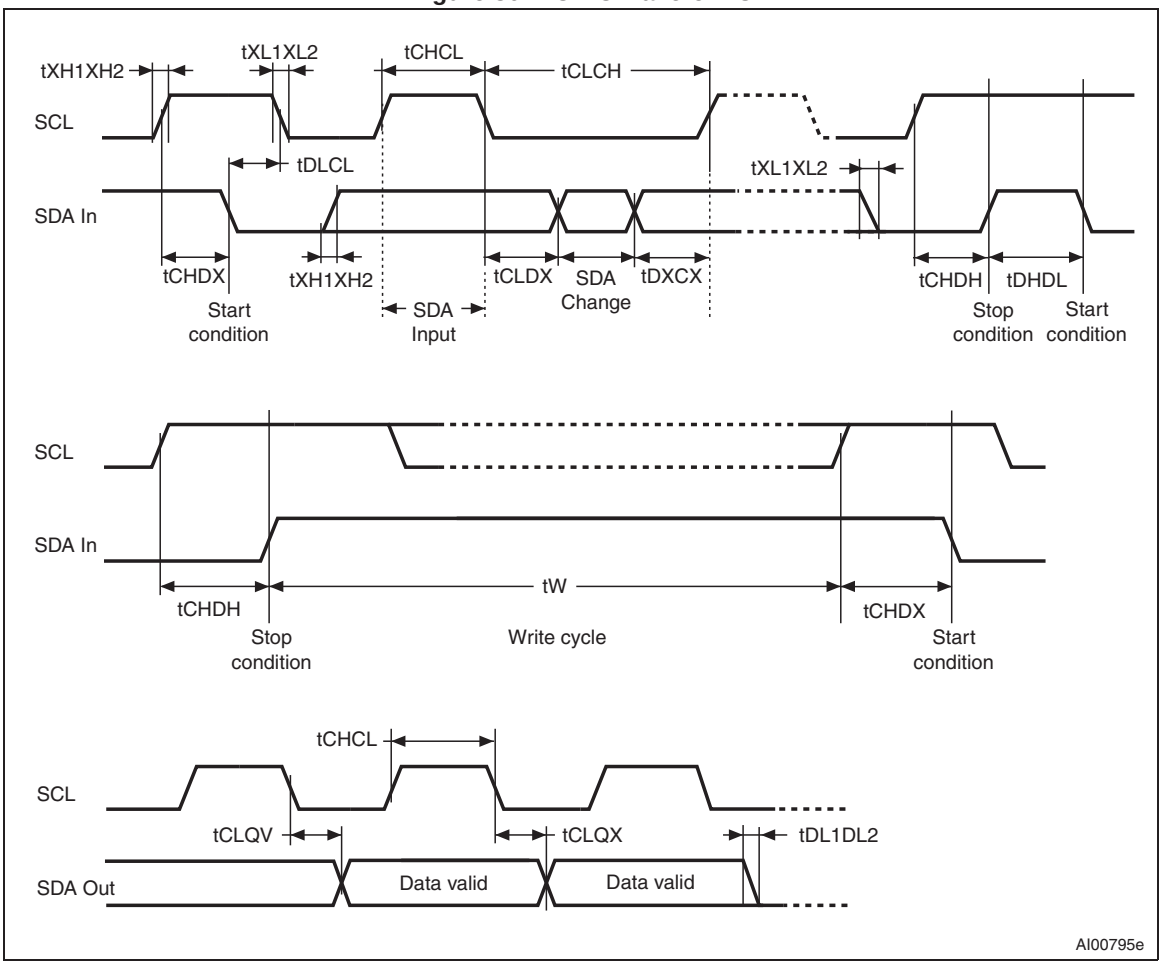
1. SCL, SDA connected to Ground or V_{CC}. SDA connected to V_{CC} through a pull-up resistor.

Table 123. I²C AC characteristics

Test conditions specified in *Table 119*					
Symbol	**Alt.**	**Parameter**	**Min.**	**Max.**	**Unit**
f_C	f_{SCL}	Clock frequency	25	400	kHz
t_{CHCL}	t_{HIGH}	Clock pulse width high	0.6	20000(1)	µs
t_{CLCH}	t_{LOW}	Clock pulse width low	1.3	20000(2)	µs
t_{START_OUT}	-	I²C timeout on Start condition	40	-	ms
t_{XH1XH2}(3)	t_R	Input signal rise time	20	300	ns
t_{XL1XL2}(3)	t_F	Input signal fall time	20	300	ns
t_{DL1DL2}	t_F	SDA (out) fall time	20	100	ns
t_{DXCX}	$t_{SU:DAT}$	Data in set up time	100	-	ns
t_{CLDX}	$t_{HD:DAT}$	Data in hold time	0	-	ns
t_{CLQX}(4)	t_{DH}	Data out hold time	100	-	ns
t_{CLQV}(5)	t_{AA}	Clock low to next data valid (access time)	100	900	ns
t_{CHDX}(6)	$t_{SU:STA}$	Start condition set up time	600	-	ns
t_{DLCL}	$t_{HD:STA}$	Start condition hold time	0.6	35000(7)	µs
t_{CHDH}	$t_{SU:STO}$	Stop condition set up time	600	-	ns
t_{DHDL}	t_{BUF}	Time between Stop condition and next Start condition	1300	-	ns
t_W	-	I²C write time	-	5	ms

1. t_{CHCL} timeout.
2. t_{CLCH} timeout.
3. Values recommended by the I²C-bus Fast-Mode specification.
4. To avoid spurious Start and Stop conditions, a minimum delay is placed between SCL=1 and the falling or rising edge of SDA.
5. t_{CLQV} is the time (from the falling edge of SCL) required by the SDA bus line to reach $0.8V_{CC}$ in a compatible way with the I²C specification (which specifies $t_{SU:DAT}$ (min) = 100 ns), assuming that the $R_{bus} \times C_{bus}$ time constant is less than 500 ns (as specified in *Figure 3*).
6. For a reStart condition, or following a write cycle.
7. t_{DLCL} timeout.

Figure 80. I²C AC waveforms



29 Write cycle definition

Table 124. Write cycle endurance(1)

Symbol	Parameter	Test conditions	Min	Max	Unit
N_{cycle}(2)	Write cycle endurance(3)	$T_A \leq +25$ °C $V_{CC(min)} < V_{CC} < V_{CC(max)}$	-	1000000	Write cycle
		$T_A \leq +85$ °C $V_{CC(min)} < V_{CC} < V_{CC(max)}$	-	150000	

1. A write cycle means the simultaneous writing of one byte, two bytes, three bytes or four bytes (one page).
2. Indicates the total number of write/erase cycles for one memory cell or the overall number of write/erase cycles decoded by the whole memory.
3. Write cycle endurance is defined by characterization and qualification.

30 RF electrical parameters

This section summarizes the operating and measurement conditions, and the DC and AC characteristics of the device in RF mode.

The parameters in the DC and AC characteristics tables that follow are derived from tests performed under the Measurement Conditions summarized in the relevant tables. Designers should check that the operating conditions in their circuit match the measurement conditions when relying on the quoted parameters.

Table 125. RF characteristics(1) (2)

Symbol	Parameter	Condition	Min	Typ	Max	Unit
f_{CC}	External RF signal frequency	-	13.553	13.56	13.567	MHz
H_ISO	Operating field according to ISO	T_A = -40 °C to 85 °C	150	-	5000	mA/m
$MI_{CARRIER}$	10% carrier modulation index(3) MI=(A-B)/(A+B)	150 mA/m > H_ISO > 1000 mA/m	15	-	30	%
		H_ISO > 1000 mA/m	10	-	30	
t_{RFR}, t_{RFF}	10% rise and fall time	-	0.5	-	3.0	µs
t_{RFSBL}	10% minimum pulse width for bit	-	7.1	-	9.44	µs
$MI_{CARRIER}$	100% carrier modulation index	MI=(A-B)/(A+B)(4)	95	-	100	%
t_{RFR}, t_{RFF}	100% rise and fall time	-	0.5	-	3.5	µs
t_{RFSBL}	100% minimum pulse width for bit	-	7	-	9.44	µs
$t_{MIN\ CD}$	Minimum time from carrier generation to first data	From H-field min	-	-	1	ms
f_{SH}	Subcarrier frequency high	$f_{CC}/32$	-	423.75	-	kHz
f_{SL}	Subcarrier frequency low	$f_{CC}/28$	-	484.28	-	kHz
t_1	Time for M24LR64E-R response	$4224/f_S$	318.6	320.9	323.3	µs
t_2	Time between commands	$4224/f_S$	309	311.5	314	µs
W_t	RF write time (including internal Verify)	-	-	5.75	-	ms
I_{CC_RF}	Operating current (Read)(5)	VAC0-VAC1 (4 V peak to peak)	-	20	-	µA
C_{TUN}	Internal tuning capacitor in SO8(6)	f = 13.56 MHz	24.8	27.5	30.2	pF
V_{BACK}	Backscattered level as defined by ISO test	ISO10373-7	10	-	-	mV
V_{MAX_1}(3)	RF input voltage amplitude between AC0 and AC1, GND pad left floating, VAC0-VAC1 peak to peak(7)	-	-	-	20	V
V_{MAX_2}(3)	AC voltage between AC0 and GND or between AC1 and GND	-	-1	-	8.5	V

Table 125. RF characteristics(1) (2) (continued)

Symbol	Parameter	Condition	Min	Typ	Max	Unit
V_{MIN_1}(3)	RF input voltage amplitude between AC0 and AC1, GND pad left floating, VAC0-VAC1 peak to peak(7)	Inventory and Read operations	-	4	4.5	V
		Write operations	-	4.5	5	V
V_{MIN_2}(3)	AC voltage between AC0 and GND or between AC1 and GND	Inventory and Read operations	-	1.8	2	V
		Write operations	-	2	2.2	V
t_{RF_OFF}	RF OFF time	Chip reset	2	-	-	ms

1. T_A = –40 to 85 °C. Characterized only.
2. All timing characterizations were performed on a reference antenna with the following characteristics:
   External size: 75 mm x 48 mm
   Number of turns: 5
   Width of conductor: 0.5 mm
   Space between two conductors: 0.3 mm
   Value of the tuning capacitor in SO8: 27.5 pF (M24LR64E-R)
   Value of the coil: 5 µH
   Tuning frequency: 13.56 MHz.
3. 15% (or more) carrier modulation index offers a better signal/noise ratio and therefore a wider operating range with a better noise immunity.
4. Temperature range 0 °C to 90 °C.
5. Characterized on bench.
6. Characterized only, at room temperature only, measured at VAC0-VAC1 = 1 V peak to peak.
7. Characterized only, at room temperature only.

Table 126. Operating conditions

Symbol	Parameter	Min.	Max.	Unit
T_A	Ambient operating temperature	-40	85	°C

Figure 81 shows an ASK modulated signal from the VCD to the M24LR64E-R. The test conditions for the AC/DC parameters are:

- Close coupling condition with tester antenna (1 mm)
- M24LR64E-R performance measured at the tag antenna
- M24LR64E-R synchronous timing, transmit and receive

Figure 81. ASK modulated signal

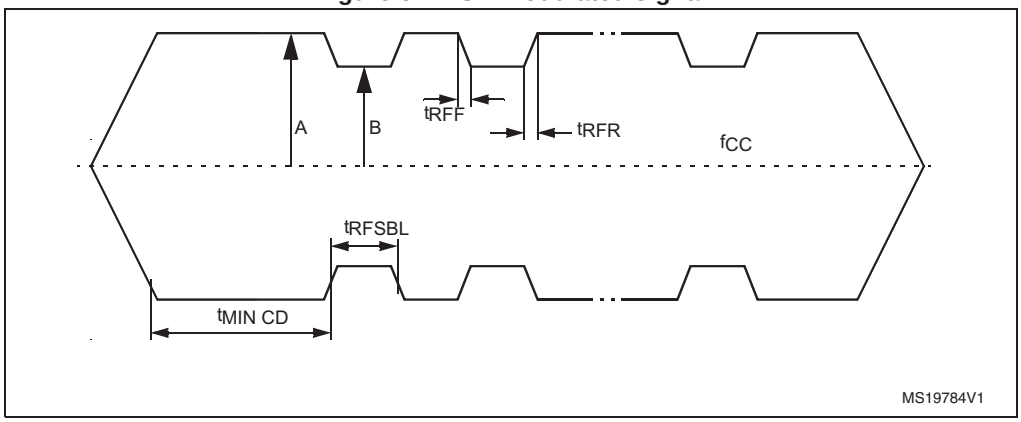


Table 127 summarizes, respectively, the minimum AC0-AC1 input power level $P_{AC0\text{-}AC1\_min}$ required for the Energy harvesting mode, the corresponding maximum current consumption I_{sink_max}, and the variation of the analog voltage V_{out} for the various Energy harvesting fan-out configurations defined by bits b0 and b1 of the Configuration byte.

Table 127. Energy harvesting(1) (2)

Range	H_{min}(3)	P_{min}(4)	V_{out}@I=0	V_{out}@I_{sink_max}	I_{sink_max}@P_{min}
00	3.5 A/m	100 mW	2.7 V min 4.5 V max	1.7 V	6 mA
01	2.4 A/m	60 mW	2.7 V min 4.5 V max	1.9 V	3 mA
10	1.6 A/m	30 mW	2.7 V min 4.5 V max	2.1 V	1 mA
11	1.0 A/m	16 mW	2.7 V min 4.5 V max	2.3 V	300 µA

1. Characterized only.
2. Valid from -40 °C to +85 °C.
3. H_{min} characterized according to ISO10373-7 test method.
4. P_{min} calculated from DC measurements.

Note: It is recommended to choose the Energy Harvesting Range according to the maximum current requested by the application to avoid any disabling of Energy Harvesting mode (for example, choose Range 01 for a max consumption of 2 mA).

Figure 82. Energy harvesting: V_{out} min vs. I_{sink}

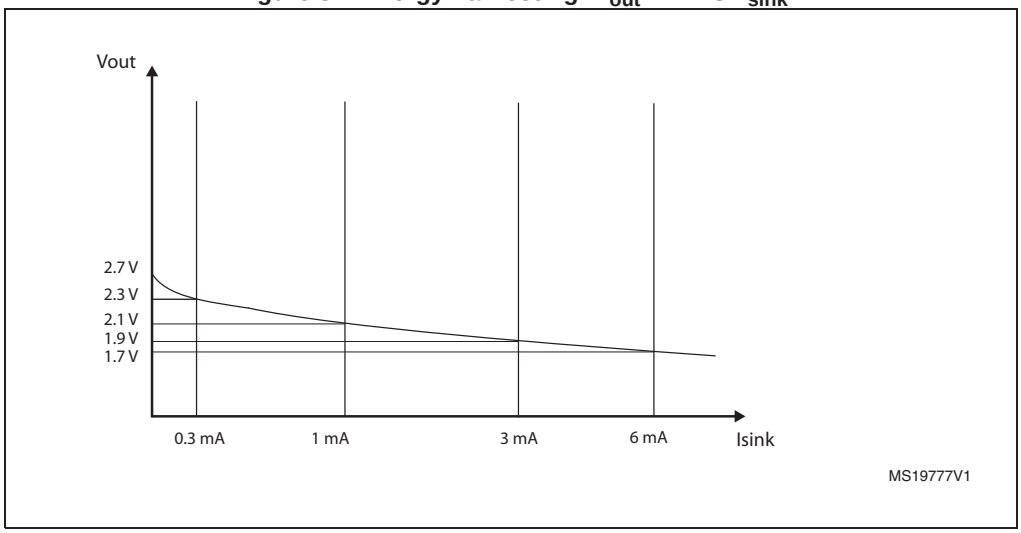


Figure 83. Energy harvesting: working domain range 11

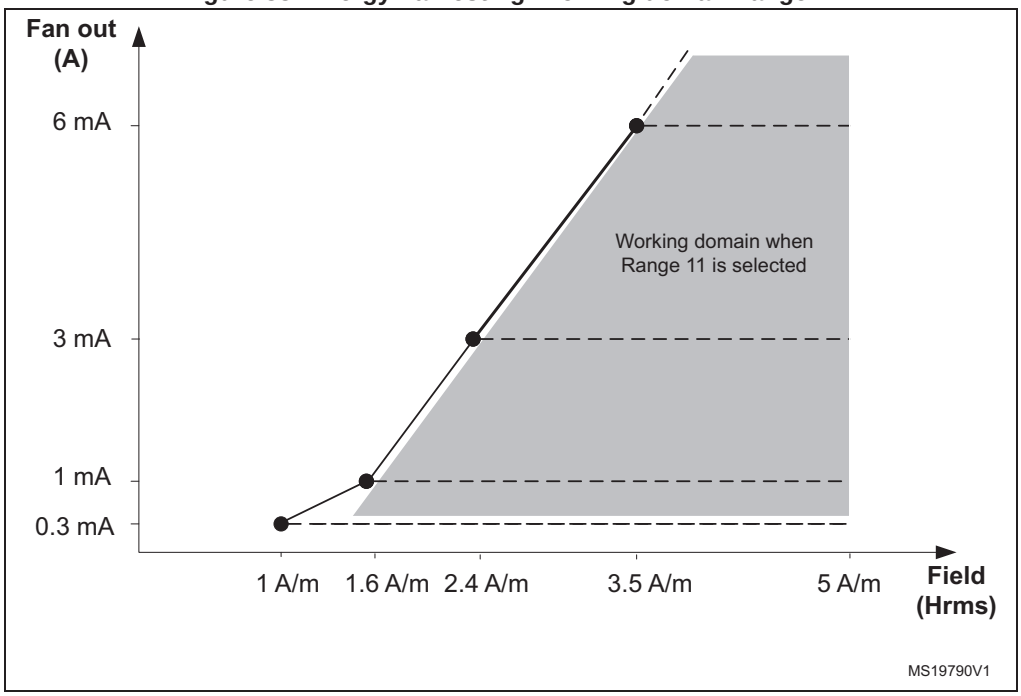


Figure 84. Energy harvesting: working domain range 10

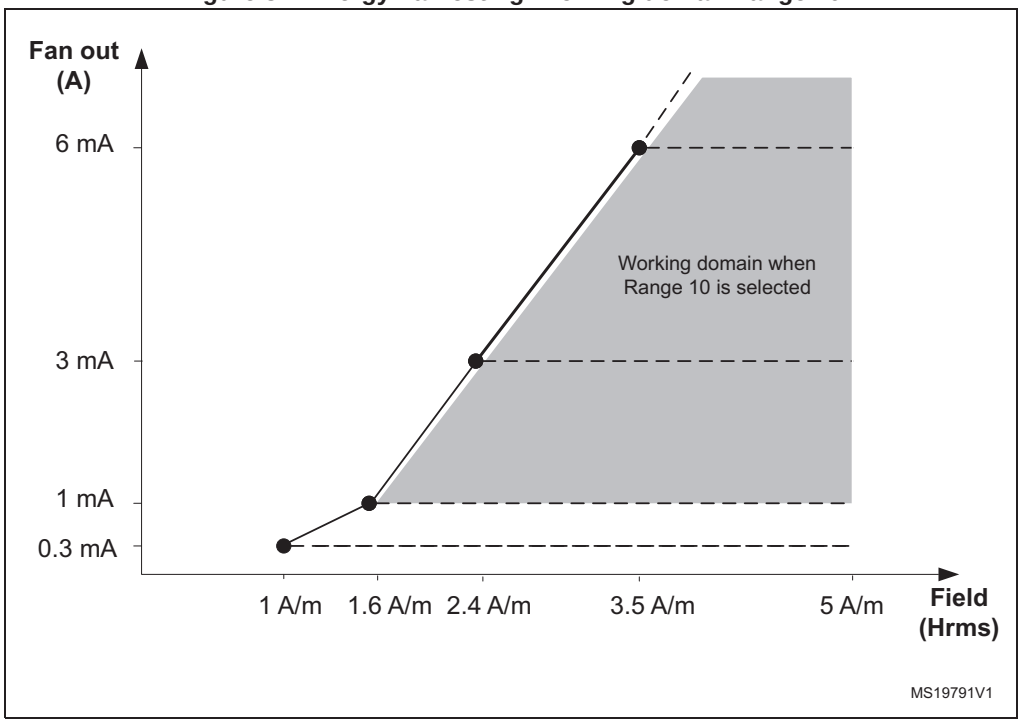


Figure 85. Energy harvesting: working domain range 01

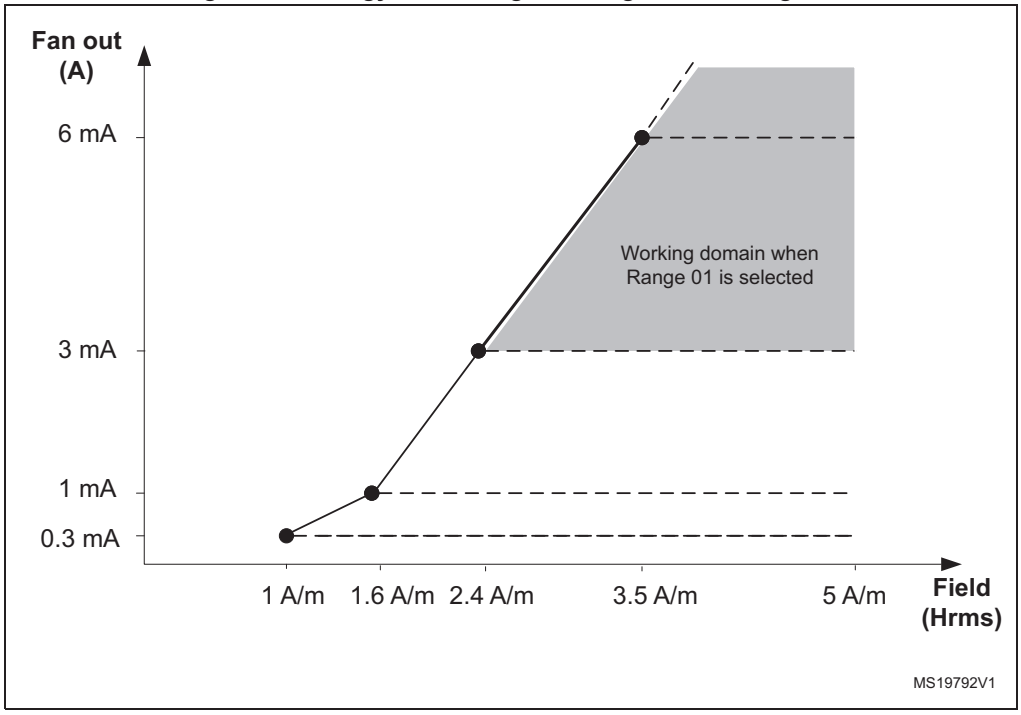
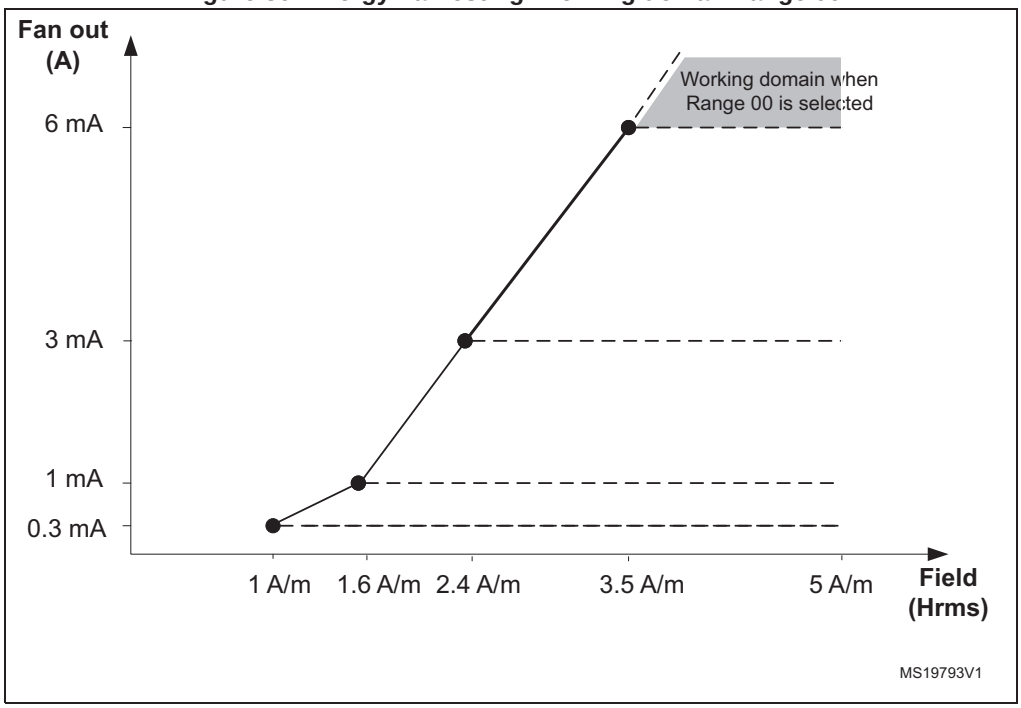


Figure 86. Energy harvesting: working domain range 00

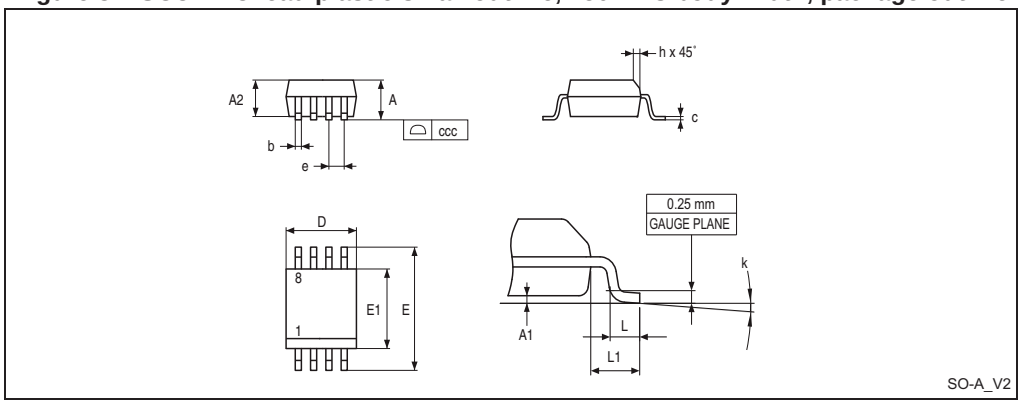


31 Package information

In order to meet environmental requirements, ST offers these devices in different grades of ECOPACK® packages, depending on their level of environmental compliance. ECOPACK® specifications, grade definitions and product status are available at: *www.st.com*. ECOPACK® is an ST trademark.

31.1 SO8N package information

Figure 87. SO8N – 8-lead plastic small outline, 150 mils body width, package outline



1. Drawing is not to scale.

Table 128. SO8N – 8-lead plastic small outline, 150 mils body width, package mechanical data

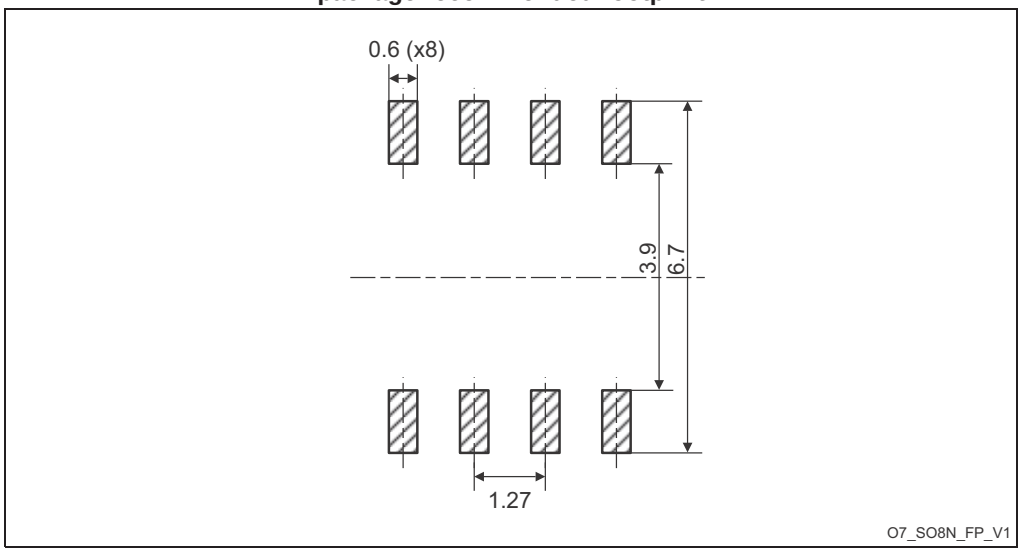
Symbol	millimeters			inches[1]		
	Min.	Typ.	Max.	Min.	Typ.	Max.
A	-	-	1.750	-	-	0.0689
A1	0.100	-	0.250	0.0039	-	0.0098
A2	1.250	-	-	0.0492	-	-
b	0.280	-	0.480	0.0110	-	0.0189
c	0.170	-	0.230	0.0067	-	0.0091
D	4.800	4.900	5.000	0.1890	0.1929	0.1969
E	5.800	6.000	6.200	0.2283	0.2362	0.2441
E1	3.800	3.900	4.000	0.1496	0.1535	0.1575
e	-	1.270	-	-	0.0500	-
h	0.250	-	0.500	0.0098	-	0.0197
k	0°	-	8°	0°	-	8°
L	0.400	-	1.270	0.0157	-	0.0500

Table 128. SO8N – 8-lead plastic small outline, 150 mils body width, package mechanical data (continued)

Symbol	millimeters			inches[1]		
	Min.	Typ.	Max.	Min.	Typ.	Max.
L1	-	1.040	-	-	0.0409	-
ccc	-	-	0.100	-	-	0.0039

1. Values in inches are converted from mm and rounded to four decimal digits.

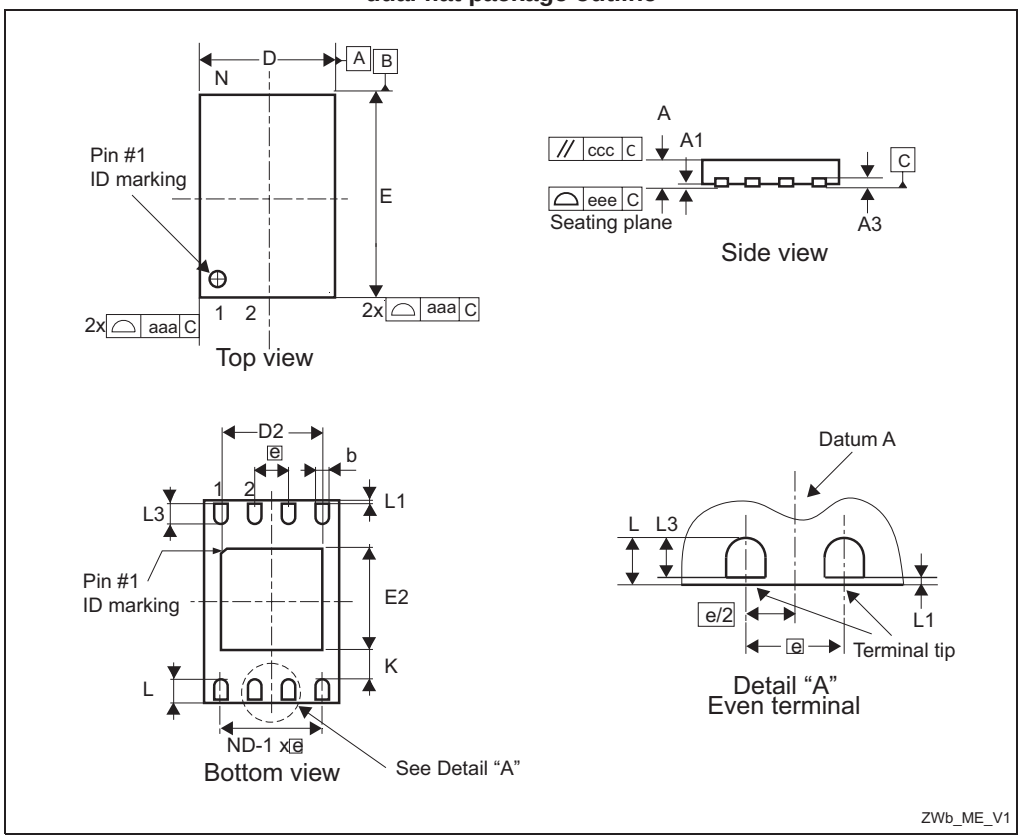
Figure 88. SO8N – 8-lead plastic small outline, 150 mils body width, package recommended footprint



1. Dimensions are expressed in millimeters.

31.2 UFDFN8 package information

Figure 89. UFDFN8 - 8-lead, 2 × 3 mm, 0.5 mm pitch ultra thin profile fine pitch dual flat package outline



1. Max. package warpage is 0.05 mm.
2. Exposed copper is not systematic and can appear partially or totally according to the cross section.
3. Drawing is not to scale.
4. The central pad (E2 by D2 in the above illustration) is internally pulled to V_{SS}. It must not be connected to any other voltage or signal line on the PCB, for example during the soldering process.

Table 129. UFDFN8 - 8-lead, 2 × 3 mm, 0.5 mm pitch ultra thin profile fine pitch dual flat package mechanical data

Symbol	millimeters			inches(1)		
	Min	Typ	Max	Min	Typ	Max
A	0.450	0.550	0.600	0.0177	0.0217	0.0236
A1	0.000	0.020	0.050	0.0000	0.0008	0.0020
b(2)	0.200	0.250	0.300	0.0079	0.0098	0.0118
D	1.900	2.000	2.100	0.0748	0.0787	0.0827
D2	1.200	-	1.600	0.0472	-	0.0630
E	2.900	3.000	3.100	0.1142	0.1181	0.1220

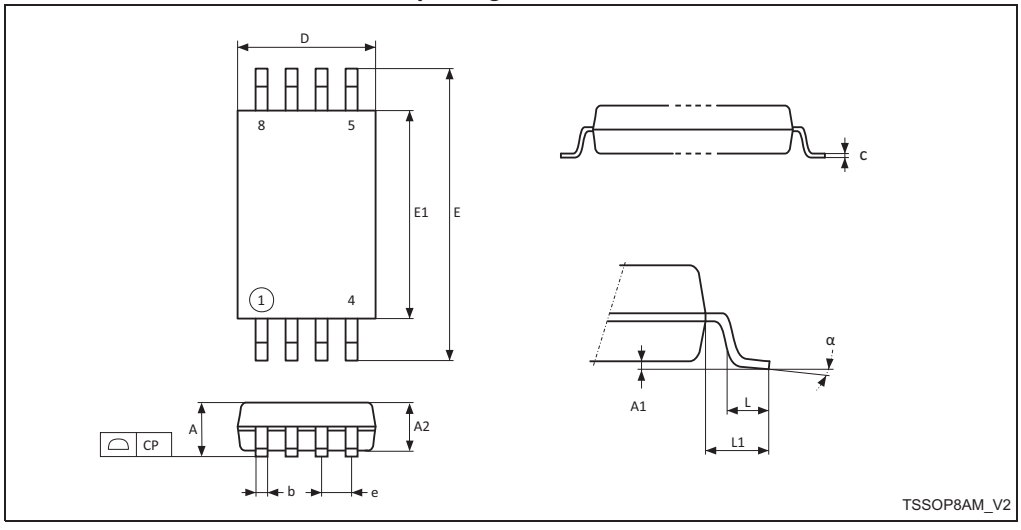
Table 129. UFDFN8 - 8-lead, 2 × 3 mm, 0.5 mm pitch ultra thin profile fine pitch dual flat package mechanical data (continued)

Symbol	millimeters			inches(1)		
	Min	Typ	Max	Min	Typ	Max
E2	1.200	-	1.600	0.0472	-	0.0630
e	-	0.500	-	0.0197		
K	0.300	-	-	0.0118	-	-
L	0.300	-	0.500	0.0118	-	0.0197
L1	-	-	0.150	-	-	0.0059
L3	0.300	-	-	0.0118	-	-
aaa	-	-	0.150	-	-	0.0059
bbb	-	-	0.100	-	-	0.0039
ccc	-	-	0.100	-	-	0.0039
ddd	-	-	0.050	-	-	0.0020
eee(3)	-	-	0.080	-	-	0.0031

1. Values in inches are converted from mm and rounded to four decimal digits.
2. Dimension b applies to plated terminal and is measured between 0.15 and 0.30 mm from the terminal tip.
3. Applied for exposed die paddle and terminals. Exclude embedding part of exposed die paddle from measuring.

31.3 TSSOP8 package information

Figure 90.TSSOP8 – 8-lead thin shrink small outline, 3 x 6.4 mm, 0.65 mm pitch, package outline



1. Drawing is not to scale.

Table 130. TSSOP8 – 8-lead thin shrink small outline, 3 x 6.4 mm, 0.65 mm pitch, package mechanical data

Symbol	millimeters			inches[1]		
	Min.	Typ.	Max.	Min.	Typ.	Max.
A	-	-	1.200	-	-	0.0472
A1	0.050	-	0.150	0.0020	-	0.0059
A2	0.800	1.000	1.050	0.0315	0.0394	0.0413
b	0.190	-	0.300	0.0075	-	0.0118
c	0.090	-	0.200	0.0035	-	0.0079
CP	-	-	0.100	-	-	0.0039
D	2.900	3.000	3.100	0.1142	0.1181	0.1220
e	-	0.650	-	-	0.0256	-
E	6.200	6.400	6.600	0.2441	0.2520	0.2598
E1	4.300	4.400	4.500	0.1693	0.1732	0.1772
L	0.450	0.600	0.750	0.0177	0.0236	0.0295
L1	-	1.000	-	-	0.0394	-
α	0°	-	8°	0°	-	8°

1. Values in inches are converted from mm and rounded to four decimal digits.

32 Part numbering

Table 131. Ordering information scheme for packaged devices

Example: M24LR64E-R MN 6 T /2

Device type

M24LR = dynamic NFC/RFID tag IC

64 = memory size in Kbit

E = support for energy harvesting

Operating voltage(1)

R = V_{CC} = 1.8 to 5.5 V

Package

MN = SO8N (150 mils width)

MC = UFDFPN8 (MLP8)

DW = TSSOP8

SB12I = 120 µm ± 15 µm bumped and sawn inkless wafer on 8-inch frame(2)

RUW20 = 725 µm ± 25 µm unsawn inkless 8-inch wafer(2)

Device grade(1)

6 = industrial: device tested with standard test flow over –40 to 85 °C

Option(1)

T = Tape and reel packing

Capacitance(1)

/2 = 27.5 pF

1. For packaged devices only.
2. Delivery type: wafer tested. Bad chip identification by STIF wafer maps available on STMicroelectronics inkless central transfer server.

Note: Parts marked as “ES”, “E” or accompanied by an Engineering Sample notification letter, are not yet qualified and therefore not yet ready to be used in production and any consequences deriving from such usage will not be at ST charge. In no event, ST will be liable for any customer usage of these engineering samples in production. ST Quality has to be contacted prior to any decision to use these Engineering samples to run qualification activity.

Table 132. Ordering and marking information

Reference	Package	Ordering code	First line marking	
			Initial revision (0xF)	Actual revision (0xE and below)
M24LR64E-R	TSSOP08	M24LR64E-RDW6T/2	464EU	4FEUB
	MLP	M24LR64E-RMC6T/2	464E	4FEB
	SO8N	M24LR64E-RMN6T/2	24L64ER	24LFERB
	SB12I	M24LR64E-SB12I/2	-	-
	RUW20	M24LR64E-RUW20/2	-	-

Appendix A Anticollision algorithm (informative)

The following pseudocode describes how anticollision could be implemented on the VCD, using recursivity.

A.1 Algorithm for pulsed slots

```
function push (mask, address); pushes on private stack
function pop (mask, address); pops from private stack
function pulse_next_pause; generates a power pulse
function store(M24LR64E-R_UID); stores M24LR64E-R_UID

function poll_loop (sub_address_size as integer)
   pop (mask, address)
   mask = address & mask; generates new mask
              ; send the request
   mode = anticollision
   send_Request (Request_cmd, mode, mask length, mask value)
   for sub_address = 0 to (2^sub_address_size - 1)
      pulse_next_pause
      if no_collision_is_detected ; M24LR64E-R is inventoried
         then
            store (M24LR64E-R_UID)
         else ; remember a collision was detected
            push(mask,address)
         endif
      next sub_address

   if stack_not_empty ; if some collisions have been detected and
      then    ; not yet processed, the function calls itself
         poll_loop (sub_address_size); recursively to process the last
stored collision
      endif
end poll_loop

main_cycle:
   mask = null
   address = null
   push (mask, address)
   poll_loop(sub_address_size)
end_main_cycle
```

Appendix B CRC (informative)

B.1 CRC error detection method

The cyclic redundancy check (CRC) is calculated on all data contained in a message, from the start of the flags through to the end of Data. The CRC is used from VCD to M24LR64E-R and from M24LR64E-R to VCD.

Table 133. CRC definition

CRC type	Length	Polynomial	Direction	Preset	Residue
ISO/IEC 13239	16 bits	$X^{16} + X^{12} + X^5 + 1 = 8408h$	Backward	FFFFh	F0B8h

To add extra protection against shifting errors, a further transformation on the calculated CRC is made. The one's complement of the calculated CRC is the value attached to the message for transmission.

To check received messages, the two CRC bytes are often also included in the re-calculation, for ease of use. In this case, the expected value for the generated CRC is the residue F0B8h.

B.2 CRC calculation example

This example in C language illustrates one method of calculating the CRC on a given set of bytes comprising a message.

C-example to calculate or check the CRC16 according to ISO/IEC 13239

```
#define  POLYNOMIAL0x8408//  x^16 + x^12 + x^5 + 1
#define  PRESET_VALUE0xFFFF
#define  CHECK_VALUE0xF0B8

#define  NUMBER_OF_BYTES4// Example: 4 data bytes
#define  CALC_CRC1
#define  CHECK_CRC0

void main()
{
  unsigned int  current_crc_value;
  unsigned char array_of_databytes[NUMBER_OF_BYTES + 2] = {1, 2, 3, 4, 0x91,
0x39};
  int           number_of_databytes = NUMBER_OF_BYTES;
  int           calculate_or_check_crc;
  int           i, j;
  calculate_or_check_crc = CALC_CRC;
// calculate_or_check_crc = CHECK_CRC;// This could be an other example
  if (calculate_or_check_crc == CALC_CRC)
  {
      number_of_databytes = NUMBER_OF_BYTES;
```

```
  }
  else    // check CRC
  {
      number_of_databytes = NUMBER_OF_BYTES + 2;
  }

  current_crc_value = PRESET_VALUE;

  for (i = 0; i < number_of_databytes; i++)
  {
      current_crc_value = current_crc_value ^ ((unsigned
int)array_of_databytes[i]);

      for (j = 0; j < 8; j++)
      {
          if (current_crc_value & 0x0001)
          {
              current_crc_value = (current_crc_value >> 1) ^ POLYNOMIAL;
          }
          else
          {
              current_crc_value = (current_crc_value >> 1);
          }
      }
  }

  if (calculate_or_check_crc == CALC_CRC)
  {
      current_crc_value = ~current_crc_value;

      printf ("Generated CRC is 0x%04X\n", current_crc_value);

      // current_crc_value is now ready to be appended to the data stream
      // (first LSByte, then MSByte)
  }
  else   // check CRC
  {
      if (current_crc_value == CHECK_VALUE)
      {
          printf ("Checked CRC is ok (0x%04X)\n", current_crc_value);
      }
      else
      {
          printf ("Checked CRC is NOT ok (0x%04X)\n", current_crc_value);
      }
  }
}
```

Appendix C Application family identifier (AFI) (informative)

The AFI (application family identifier) represents the type of application targeted by the VCD and is used to extract from all the M24LR64E-Rs present only the one meeting the required application criteria.

It is programmed by the M24LR64E-R issuer (the purchaser of the M24LR64E-R). Once locked, it cannot be modified.

The most significant nibble of the AFI is used to code one specific or all application families, as defined in *Table 134*.

The least significant nibble of the AFI is used to code one specific or all application subfamilies. Subfamily codes different from 0 are proprietary.

Table 134. AFI coding(1)

AFI most significant nibble	AFI least significant nibble	Meaning VICCs respond from	Examples / Note
‘0’	‘0’	All families and subfamilies	No applicative preselection
‘X’	'0	All subfamilies of family X	Wide applicative preselection
'X	''Y’	Only the Yth subfamily of family X	-
‘0’	‘Y’	Proprietary subfamily Y only	-
‘1	‘‘0’, ‘Y’	Transport	Mass transit, bus, airline,...
'2	‘‘0’, ‘Y’	Financial	IEP, banking, retail,...
'3	‘‘0’, ‘Y’	Identification	Access control,...
'4	‘‘0’, ‘Y’	Telecommunication	Public telephony, GSM,...
‘5’	‘0’, ‘Y’	Medical	-
'6	‘‘0’, ‘Y’	Multimedia	Internet services....
'7	‘‘0’, ‘Y’	Gaming	-
8	‘‘0’, ‘Y’	Data Storage	Portable files,...
'9	‘‘0’, ‘Y’	Item management	-
'A	‘‘0’, ‘Y’	Express parcels	-
'B	‘‘0’, ‘Y’	Postal services	-
'C	‘‘0’, ‘Y’	Airline bags	-
'D	‘‘0’, ‘Y’	RFU	-
'E	‘‘0’, ‘Y’	RFU	-
‘F’	‘0’, ‘Y’	RFU	-

1. X = '1' to 'F', Y = '1' to 'F'

Revision history

Table 135. Document revision history

Date	Revision	Changes
12-Apr-2012	1	Initial release.
08-Jun-2012	2	Updated *Section 7.1: RF communication and energy harvesting on page 42* and *Figure 49: M24LR64E-R state transition diagram on page 65*. Updated clock pulse width values in *Table 123: I^2C AC characteristics on page 122*.
19-Jun-2012	3	Updated notes for *Figure 49: M24LR64E-R state transition diagram*.
21-Feb-2013	4	– Number of sectors updated in *Section 3*. – Updated *Section 4.2*. – Updated *Figure 6: Memory sector organization*. – M24LR64E changed into M24LR64x in *Figure 52: M24LR64E RF-Busy management following Inventory command*, *Figure 56: M24LR64E RF-Busy management following Write command* and *Figure 57: M24LR64E RF-Wip management following Write command*. – Updated *Table 15: Control register*, *Table 17: System parameter sector*, *Table 118: Absolute maximum ratings*, *Table 122: I^2C DC characteristics* and *Table 125: RF characteristics*.
07-Mar-2013	5	Added *Table 132: Ordering and marking information*.
12-Jun-2013	6	Added “Dynamic NFC/RFID tag IC” to the title, *Section 1: Description*, and the M24LR definition in *Table 131: Ordering information scheme for packaged devices*. Updated V_{ESD} and Note 5 in *Table 118: Absolute maximum ratings*. Removed MB package from *Figure 88: UFDFPN8 (MLP8) – 8-lead ultra thin fine pitch dual flat package no lead 2 × 3mm, package outline*.
21-Nov-2014	7	Updated *Figure 1: Logic diagram*, *Figure 14: 100% modulation waveform* and *Figure 15: 10% modulation waveform*. Updated footnote *4* in *Table 123: I^2C AC characteristics*. Added note on Engineering samples marking in *Section 32: Part numbering*.
06-Nov-2015	8	Updated figure on Cover page with new wafer code SB12I. Updated *Figure 10: Write cycle polling flowchart using Ack*, *Figure 14: 100% modulation waveform* and *Figure 15: 10% modulation waveform*. Updated *Table 118: Absolute maximum ratings* and its footnote *4*. Updated *Section 31: Package information* and its subsections. Updated *Table 131: Ordering information scheme for packaged devices* and added footnotes *1* and *2*.
27-Apr-2016	9	Updated *Table 132: Ordering and marking information*.
09-May-2016	10	Updated *Features*. Updated *Figure 51: Description of a possible anticollision sequence* and *Figure 53: Stay Quiet frame exchange between VCD and M24LR64E-R*. Updated *Table 118: Absolute maximum ratings*. Added *Section 29: Write cycle definition*.

Table 135. Document revision history (continued)

Date	Revision	Changes
13-Mar-2017	11	Updated image on cover page with introduction of RUW20 wafer option. Updated *Features*. Added footnote *4* to *Figure 89: UFDFN8 - 8-lead, 2 × 3 mm, 0.5 mm pitch ultra thin profile fine pitch dual flat package outline*. Updated *Table 131: Ordering information scheme for packaged devices* and *Table 132: Ordering and marking information*.
20-Jul-2017	12	Updated caption of *Figure 90: TSSOP8 – 8-lead thin shrink small outline, 3 x 6.4 mm, 0.65 mm pitch, package outline* and of *Table 130: TSSOP8 – 8-lead thin shrink small outline, 3 x 6.4 mm, 0.65 mm pitch, package mechanical data*.

IMPORTANT NOTICE – PLEASE READ CAREFULLY

STMicroelectronics NV and its subsidiaries (“ST”) reserve the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice. Purchasers should obtain the latest relevant information on ST products before placing orders. ST products are sold pursuant to ST’s terms and conditions of sale in place at the time of order acknowledgement.

Purchasers are solely responsible for the choice, selection, and use of ST products and ST assumes no liability for application assistance or the design of Purchasers’ products.

No license, express or implied, to any intellectual property right is granted by ST herein.

Resale of ST products with provisions different from the information set forth herein shall void any warranty granted by ST for such product.

ST and the ST logo are trademarks of ST. All other product or service names are the property of their respective owners.

Information in this document supersedes and replaces information previously supplied in any prior versions of this document.

EXHIBIT E

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

TRIDINETWORKS LTD., Plaintiff, v. NXP-USA, INC. and NXP B.V., Defendants.	No. 1:19-01062-CFC-CJB
TRIDINETWORKS LTD., Plaintiff, v. SIGNIFY NORTH AMERICA CORPORATION and SIGNIFY NETHERLANDS B.V., Defendants.	No. 1:19-01063-CFC-CJB
TRIDINETWORKS LTD., Plaintiff, v. STMICROELECTRONICS, INC., and STMICROELECTRONICS INTERNATIONAL N.V., AND DOE-1 d/b/a "STMICROELECTRONICS," Defendants.	No. 1:19-01064-CFC-CJB

REBUTTAL DECLARATION OF MICHAEL CALOYANNIDES, PH.D. CONCERNING THE CONVENTIONAL APPLICATION OF COMPUTER TECHNOLOGY IN THE CLAIMS OF THE '276 PATENT

commissioning tool . . . through the configuration link 207." '276 Patent 14:49-52. In other words, the configuration interface transfers configuration data. This is exactly what an interface is expected to do. The '276 Patent explains that this "data load may be carried out by contactless technologies (such as RFID/NFC)." '276 Patent 14:58-60. This is to be expected because RFID/NFC is a conventional computer technology for implementing a contactless data transfer interface. In other words, configuration interface 702 is a conventional computer interface performing conventional interface functions.

59. In summary, "configuration adapter" is just a name the '276 Patent gives to a group of conventional computer components conventionally transferring data. They operate exactly the same when transferring configuration data as they do when transferring any other kind of data.

D. A Device or Technology May Be Conventional Even Though a Particular Part is Not Available Off-the-Shelf.

60. Dr. Rowe argues that configuration adapters as described in the '276 Patent were not conventional because, "[i]n 2007, such items were not generally available off-the-shelf." Rowe Decl. ¶ 62 (emphasis added). Here, Dr. Rowe is confusing conventional technology with off-the-shelf parts. These are two different concepts, and one may not imply the other.

61. A conventional technology is one that is in common use. RFID was a conventional technology in November 2007. It was standardized and used by many companies in different industries for a variety of applications.

62. Off-the-shelf parts are available as stock items, not specifically designed or customized for a particular buyer. Off-the-shelf parts commonly implement conventional technologies, but conventional technologies are not restricted to off-the-shelf parts.

63. Companies may design custom parts to implement conventional technologies (or conventional device types) for a variety of reasons that have nothing to do with, and change nothing about, the underlying technology (or the operation of the device). For example, a company may need a part with a specific form factor or layout to fit a product with an unusual size or shape. Alternatively, a company may need a part packaged in a unique material to resist environmental conditions, like excess temperature, moisture, or pressure. Alternatively, a company may need a part with a unique shape or connector to accommodate its manufacturing and assembly processes. Alternatively, a part may be designed for use in a highly regulated industry or by specially authorized entities, such as military or aerospace contractors. In each case, the underlying technology and device type of the part may be conventional even though the individual part designs may never be made available off-the-shelf.

64. There are many considerations that go into designing and packaging a modern electronic component. A few examples include:

- Size and layout (e.g., parts for use in a modern smartphone are typically thin and laid out horizontally, whereas parts for other applications may be laid out with a smaller horizontal footprint and an extended vertical dimension);
- Connection type (e.g., ball grid array, land grid array, dual in-line pins, etc.);
- Package material (e.g., resin, plastic, ceramic);
- Package characteristics (e.g., thermal conductivity, electrical insulation, RF transparency, heat resistance, moisture resistance, UV resistance, chemical resistance, flexibility, rigidity, etc.);
- Cooling type (passive vs. active); and
- Integration (i.e., whether the part will provide a stand-alone function or combine multiple functions).[14]

65. To better understand the issue, consider cell phones. In the early 2000s, cell phones came in many different shapes and sizes: mini brick, clamshell, slider. Although they all shared many of the same, conventional technologies, a part

[14] Integration is a hallmark of modern electronics.

designed for one phone manufacturer might not fit or work in a cell phone made by a different manufacturer. This is even true today when cell phones made by different manufacturers look remarkably similar. Individual manufacturers customize parts, changing layout, packaging materials, connectors, etc. to make space for new features, bigger batteries, or simply slimmer phones. Even when those parts implement the same conventional technologies used by competitors, they may not be offered off-the-shelf because the space-saving design of the part is specific or proprietary to one manufacturer. In that case, both the technology and the type of part may be conventional across the industry, but each manufacturer is supplied an exclusive part with a design and layout customized to its own phone.

66. In other words, the absence of an off-the-shelf part for a particular application does not mean that the underlying technology or the application itself is unconventional. On the contrary, a technology may be considered conventional before it ever becomes available in an off-the-shelf part. This is true because the availability of off-the-shelf parts is determined by many factors beyond whether a technology is or has become conventional.

E. The Prior Art Shows the Gradual Adoption of Devices Matching the Features, Function, and Operation of Configuration Adapters from December 2001 to August 2006.

67. As discussed in my previous declaration, prior art patents show that many multinational companies were incorporating devices matching the features, function, and operation[15] of configuration adapters into their products. In some cases, these devices were incorporated specifically for the purpose of network configuration – exactly the same purpose[16] as the configuration adapters of the '276 Patent.

---

[15] To avoid ambiguity, when I refer to "the same features, functions, [and] operations" or use similar language, I am referring to the functional elements and operational characteristics attributed to a configuration adapter in the specification of the '276 Patent, specifically: an RFID/NFC interface, a wired interface for communication with a host device, a control and memory element, the ability to receive and store data via the RFID/NFC interface without being supplied with power by the host device, and the ability to retain data without a continuous supply of power (non-volatile memory).

[16] When I refer to the "application" or "use" or "purpose" of a device in comparison to a configuration adapter of the '276 Patent, I am referring, generally,

68. Whether those companies were purchasing these devices as off-the-shelf parts or assembling the devices themselves from other conventional computer components is irrelevant. The prior art patents show how devices of this type were being constructed and used before November 2007.

69. When viewed together, the prior art patents discussed in my opening declaration map out a timeline showing the adoption of these devices by major international companies for various applications – including network configuration applications – over the period from December 2001 to August 2006. In other words, they show the device being adopted and becoming a conventional computer component before November 2007.

70. For example, the Spencer Patent disclosed a dual-interface, RFID memory device matching the features, functionality, and operation of the configuration adapter of the '276 Patent, although a use for device configuration was not disclosed. Caloyannides Opening Decl. ¶¶ 156 – 168. The Spencer Patent was filed on December 5, 2001 and assigned to Hewlett-Packard.

71. The Teraura Patent disclosed a similar dual-interface, RFID memory device matching the features, function, and operation of the configuration adapter of

---

to the type of data it is being used to receive and store or to the intended use for that data.

the ’276 Patent, although a use for device configuration was not disclosed. Caloyannides Opening Decl. ¶¶ 169 – 174. The Teraura Patent arose from applications filed in August 2001 and July 2002 and issued in March 2005. It was assigned to Denso Corporation, an international auto parts manufacturer.

72. The Dua Patent discloses a similar dual-interfaced, RFID memory device matching the features, functionality, and operation of the configuration adapter of the ’276 Patent. Dua specifically discloses the use of this device for establishing network connections between devices. The Dua Patent arose from an application filed in May 2005 and published in November 2006.

73. The Smith Patent discloses a dual-interface, RFID memory device matching the features, functionality, and operation of the configuration adapter of the ’276 Patent. Smith specifically discloses the use of this device for device configuration, including network configuration. Caloyannides Opening Decl. ¶¶ 176 – 185. The Smith Patent arose from an application filed in August 2006 and was assigned to Intel Corporation.

F. Computers vs. Components

74. Dr. Rowe appears to draw a distinction between fully assembled computers and the conventional components of computer and computer technology. For example, Dr. Rowe states that “the configuration adapter is in no way a computer” in part because it “is not a device that computes or controls anything, or whose

internal operation or state is controlled by software or programs." Rowe Decl. ¶ 52. Dr. Rowe's analysis misses the point in several respects.

75. First, Dr. Rowe simply mischaracterizes the configuration adapter of the '276 Patent. The specification of the '276 Patent explains that the configuration adapter includes a "control and memory module 700" that "may be used to store the loaded configuration data and **to control the adapter**." '276 Patent 14:60-61 (emphasis added). In other words, the specification directly contradicts Dr. Rowe's analysis.

76. Dr. Rowe's comments also misinterpret my analysis. Put simply, my opinion is that a configuration adapter is a conventional component of computer technology. It is assembled from conventional components of computer technology. The operations performed by the configuration adapter in the context of the '276 Patent – downloading data, storing data, reading data – are merely the conventional operations performed by such a component in whatever computer system incorporates it.

VII. Dr. Rowe's Exhibits

A. Product Data Sheets

77. Dr. Rowe relies on one product data sheet from NXP and one product data sheet and one product announcement from STMicroelectronics to argue that configuration adapters "did not appear on the market until approximately 2010."

Rowe Decl. ¶ 62 and Exhibits D, E, F. At most, these documents show when specific product models came onto the market. They do not establish when configuration adapters first entered the market or became conventional.

78. For example, Philips Semiconductors released a specification, revision 2.0, in February 2004 for a PN531 μC (microcontroller) based transmission module.[17] (I understand Philips Semiconductors to be a predecessor of NXP.) A diagram of the device shows it has all of the same components as the configuration adapter of the ’276 Patent:

[17] A copy of this document is provided as Exhibit A to this declaration.

2 BLOCK DIAGRAM

2.1 Simplified PN531 Block Diagram

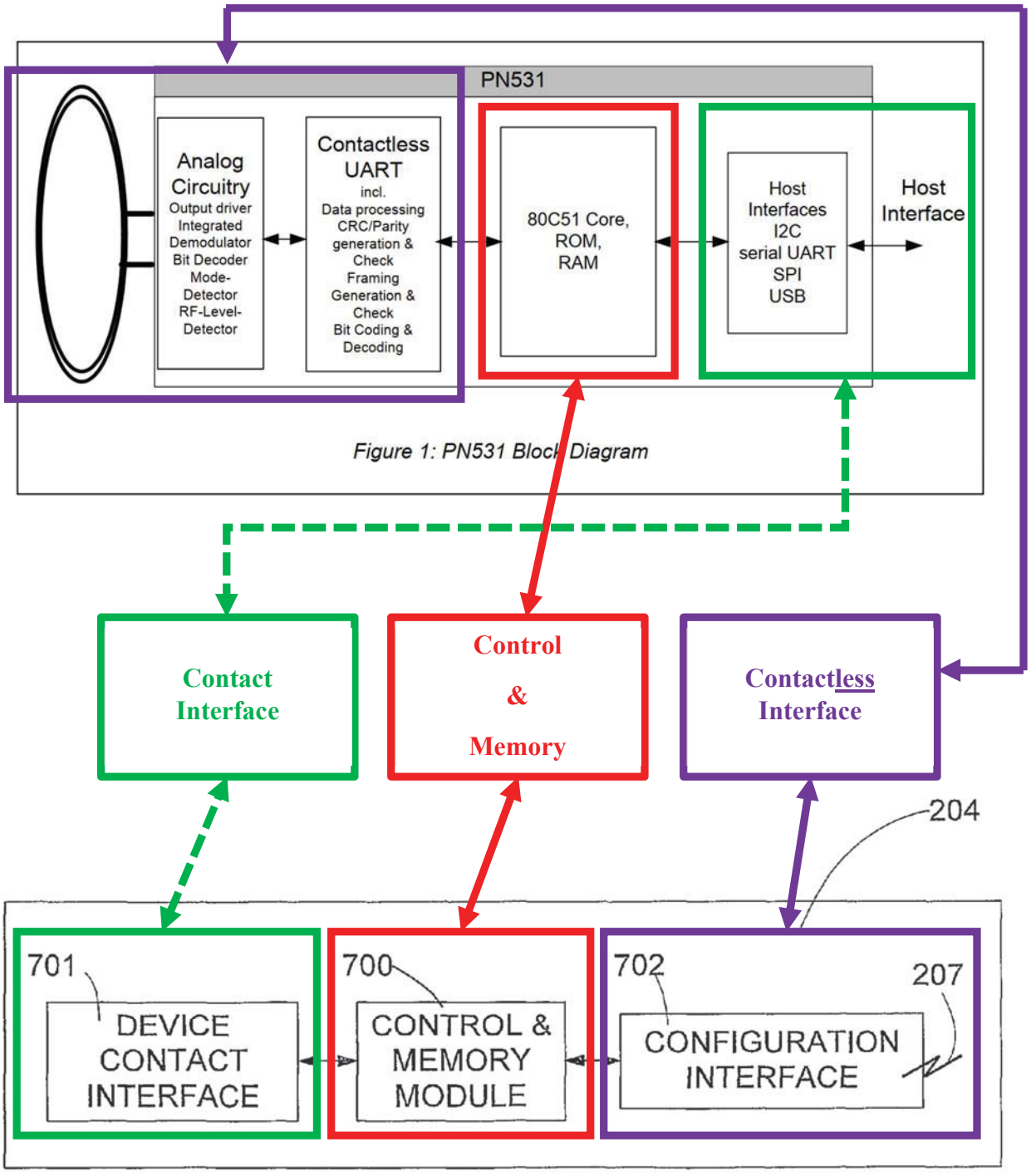


Fig. 7

79. It is worth noting that, although the Philips product specification says nothing about using the PN531 device to receive and store configuration data, Philips was publishing other materials in 2004 that specifically suggest this use. In particular, Philips published a presentation with a 2004 copyright date that specifically states that "NFC can also bootstrap other wireless protocols like Bluetooth or Wireless Ethernet (WiFi) by **exchanging configuration and session data**." Philips Presentation, page 16 (emphasis added). One of the products discussed in this presentation is the "PN531 Smart Transmission Module," Philips Presentation, pages 16, 22, the same module discussed above.

B. NASA Tech Brief

80. Dr. Rowe argues that a short article published in NASA Tech Briefs "captures the RFID zeitgeist" and demonstrates that the capabilities of RFID storage devices were not appreciated as of May 2007. Rowe Decl. ¶ 66 and Exhibit G. Dr. Rowe gives far too much weight to one paragraph in this article.

81. First, the entire article is only one page long,[18] and it contains only one paragraph discussing the state of the art in RFID. Rowe Decl., Exhibit G, at 6. This

[18] It begins part way through one page and continues on the next, but it clearly appears that it could have been printed on a single page.

C. ZigBee Wireless Networking Book

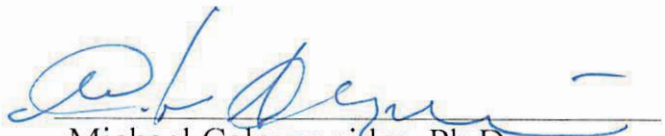
84. Dr. Rowe relies on a book about ZigBee wireless networking to draw conclusions about the state of the art concerning RFID. Rowe Decl. ¶ 66 and Exhibit H. This book is an inappropriate reference to show the RFID state of the art. The book was published by the ZigBee Alliance, and its "Intended Audience" is "developers who are interested in learning more about ZigBee." Rowe Decl., Exhibit H, at xi ("Preface"). It is unsurprising to me that the book does not address RFID.

VIII. Conclusion

85. The foregoing represents my opinions to date, but I reserve the right to supplement my opinions in response to arguments raised in opposition to this declaration or if further evidence or information becomes available.

86. I declare under penalty of perjury that the foregoing is true and correct.

Dated: December 30, 2020



Michael Caloyannides, Ph.D.

EXHIBIT F

Short Form Specification

Near Field Communication

PN531- µC based Transmission module

Objective Short Form Specification

February 2004

Revision 2.0

Public

Philips
Semiconductors

PHILIPS

PN531 **µC based Transmission module**

CONTENTS

1 INTRODUCTION

1.1 Scope

The PN531 is a highly integrated transmission module for contactless communication at 13.56 MHz including µ-controller functionality based on an 80C51 core with 32 kbyte of ROM and 1 kbyte of RAM. This µc-based transmission module combines an outstanding modulation and demodulation concept completely integrated for different kinds of contactless communication methods and protocols at 13.56 MHz with an easy to use firmware for the different supported modes and the required host interfaces.

The embedded firmware handles the ISO 14443A and MIFARE® reader protocol as well as the basic FeliCa™ reader protocol and the complete NFC IP-1 protocol.
Furthermore the embedded firmware and the internal hardware support the handling and the host protocols for the different interfaces as

- USB 2.0
- I2C
- SPI and
- Serial UART

The PN531 supports 3 different operating modes

- Reader/writer mode for FeliCa™ and ISO14443A cards
- Supports Card interface mode for FeliCa™ and ISO14443A/MIFARE® in combination with secure µC
- NFC IP-1 mode

In reader/ writer mode the PN531's internal transmitter part is able to drive a reader/writer antenna designed to communicate with ISO14443A /MIFARE® or FeliCa™ cards and transponders without additional active circuitry. The receiver part provides a robust and efficient implementation of a demodulation and decoding circuitry for signals from ISO14443A compatible cards and transponders. The digital part handles the complete ISO14443A framing and error detection (Parity & CRC).

The PN531 supports MIFARE® Classic (e.g. MIFARE® Standard) products. The PN531 supports contactless communication using MIFARE® Higher Baudrates up to 424kbit/s in both directions. In the reader/ writer mode the PN531 transmission module supports the FeliCa™ communication scheme. The receiver part provides a robust and efficient implementation of the demodulation and decoding circuitry for FeliCa™ coded signals. The digital part handles the FeliCa™ framing and error detection like CRC.

The PN531 supports contactless communication using FeliCa™ Higher Baudrates up to 424kbit/s in both directions.

In card mode the PN531 is able to answer a reader/writer command either in FeliCa™ or ISO14443A/MIFARE® card mode. The PN531 generates the proper digital load modulated signals and with an external circuit, can respond to commands sent by the reader/writer.

The PN531 offers the possibility to directly communicate with several NFC enabled devices in the NFC IP-1 mode. The NFC IP-1 mode offers different baudrates up to 424kbit/s. The PN531 handles the complete NFC framing and error detection.

1.1 Features

- 80C51 microcontroller core with 32 kbyte ROM and 1 kbyte RAM
- Highly integrated analog circuitry for transmission and reception
- Output drivers to connect an antenna with minimum number of external components
- Integrated RF Level detector
- Integrated mode detector
- Hardware and embedded Firmware support for
  - ISO 14443A reader/writer mode
  - MIFARE® Classic encryption and MIFARE® higher baudrate communication up to 424 kbit/s
  - Contactless communication according to the FeliCa™ scheme at 212 kbit/s and 424 kbit/s
  - NFC standard ECMA 340 and ISO 18092: NFC IP-1 interface and protocol
  - Host protocol on following interfaces
    - USB 2.0 full speed compliant device
    - SPI
    - I2C
    - High speed serial UART
- Optional interrupt line to the host
- Hard reset with low power function
- Flexible Power down mode or power reduction mode per software
- Internal oscillator to connect a 27.12 MHz quartz
- Internal oscillator to connect a 4 MHz quartz for the USB interface
- 2.5 - 3.6 V power supply
- USB bus powered (In USB mode)
- Specific IO ports and interrupt sources for external devices control

1.2 Application

The PN531 is tailored to fulfil the requirements of various applications using contactless communication based on the ECMA340 (NFC IP-1) Interface and protocol standard, the ISO14443A reader and FeliCa reader protocol. NFC IP-1 is also standardised in ISO/IEC 18092.
Compatible to current RFID infrastructure the NFC technology offers a new direct communication link between two NFC enhanced devices. This peer-to-peer communication enables a direct data exchange between devices.
The integrated microcontroller and embedded firmware of the PN 531 means a fast and easy integration in a contactless system. The high-level abstraction commands and the complete handling of RF communication protocols free the host CPU of all real time related constraints.

NFC technology is designed to meet requirements for consumer markets, as well as handheld and PC markets.

Typical devices to integrate the PN531 are

- Mobile phones
- PDAs
- PCs
- Intelligent remote controls
- PC peripherals e.g. printers and mice
- Consumer electronic devices like digital cameras

2 BLOCK DIAGRAM

2.1 Simplified PN531 Block Diagram

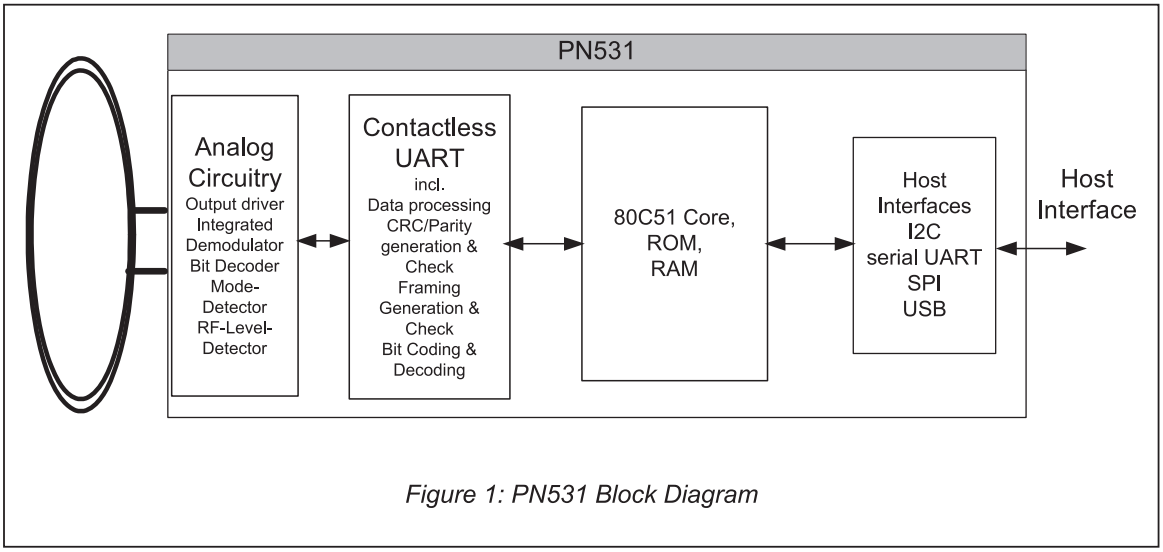


Figure 1: PN531 Block Diagram

The Analog circuitry handles the modulation and demodulation of the analog signals according to the card mode, reader /writer mode and NFC mode communication scheme.

The RF level detector detects the presence of an external RF field at 13.56 MHz.

The mode detector detects a MIFARE®, FeliCa™ or NFC coding of an incoming signal in order to prepare the internal receiver to demodulate signals that are sent to the PN531.

The integrated contactless UART and the firmware handle the protocol requirements for the communication schemes including the RF based protocols as well as the protocols for host communication.
The microcontroller with its embedded firmware allows autonomous management of communication both on the RF interface and with the host.

Various host interfaces are implemented to fulfil different customer requirements.

3 PN531 PINNING INFORMATION

3.1 Pinning Diagram

The device is available in an HVQFN40 package.

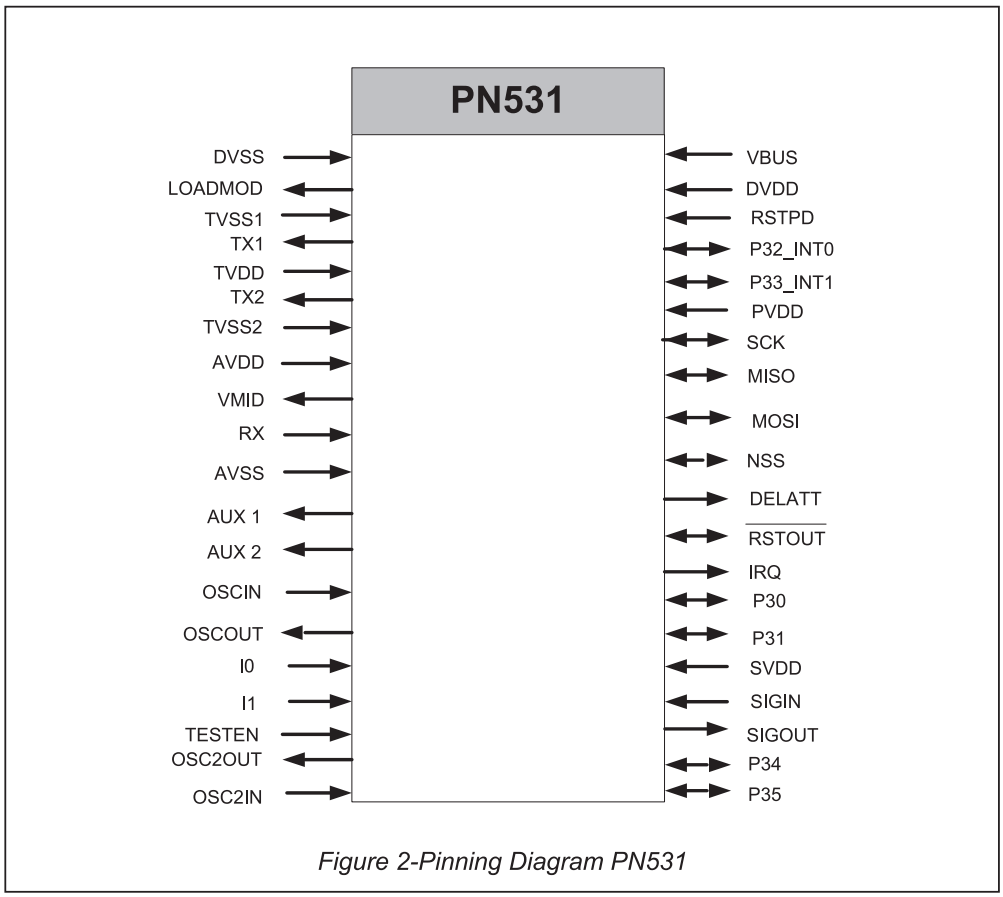


Figure 2-Pinning Diagram PN531

The device operates with six individual power supplies for best performance in terms of EMC behaviour and signal de-coupling. This gives outstanding RF performance and maximum flexibility to adapt to different operating voltages of digital and analog parts.

3.2 Pin Description

Pin	Symbol	Type	Pad Ref Voltage	Description
1	DVSS	PWR		Digital Ground
2	LOADMOD	O	DVDD	Load Modulation output provides digital signal for FeliCa and MIFARE® card operating mode
3	TVSS1	PWR		Transmitter Ground: supplies the output stage of TX1 and TX2
4	TX1	O	TVDD	Transmitter 1: delivers the modulated 13.56 MHz energy carrier
5	TVDD	PWR		Transmitter power supply: supplies the output stage of TX1 and TX2
6	TX2	O	TVDD	Transmitter 2: delivers the modulated 13.56 MHz energy carrier
7	TVSS2	PWR		Transmitter Ground: supplies the output stage of TX1 and TX2
8	AVDD	PWR		Analog Power Supply
9	VMID	PWR	AVDD	Internal Reference Voltage: This pin delivers the internal reference voltage.
10	RX	I	AVDD	Receiver Input: Input pin for the reception signal, which is the load modulated 13.56 MHz energy carrier from the antenna circuit.
11	AVSS	PWR		Analog Ground
12	AUX1	O	DVDD	Auxiliary Output: This pin delivers analog and digital test signals.
13	AUX2	O	DVDD	Auxiliary Output: This pin delivers analog and digital test signals.
14	OSCIN	I	AVDD	Crystal Oscillator Input: input to the inverting amplifier of the oscillator. This pin is also the input for an externally generated clock (fosc = 27.12 MHz).
15	OSCOUT	O	AVDD	Crystal Oscillator output: Output of the inverting amplifier of the oscillator.
16	I0	I	DVDD	Interface mode lines: selects the used host interface. In test mode I0 is used as test signals.
17	I1	I	DVDD	Interface mode lines: selects the used host interface. In test mode I0 is used as test signals.
18	TESTEN	I	DVDD	Test enable pin: When set to 1 enable the test mode. When set to 0 reset the TCB and disable the access to the test mode.
19	OSC2OUT	O	DVDD	Crystal Oscillator output: Output of the inverting amplifier of the oscillator for the USB clock.
20	OSC2IN	I	DVDD	Crystal Oscillator Input: input to the inverting amplifier of the oscillator for the USB clock generation. This pin is also the input for an externally generated clock (f_{osc} =4 MHz). In test mode this signal is used as test clock input
21	P35	IO	DVDD	General purpose IO signal
22	P34	IO	SVDD	General purpose IO signal or clk signal for the SAM
23	SIGOUT	O	SVDD	Contactless communication interface output: delivers a serial data stream according to NFCIP-1 and output signal for the SAM. In test mode this signal is used as test signal output.
24	SIGIN	I	SVDD	Contactless communication interface input: accepts a digital, serial data stream according to NFCIP-1 and input signal from the SAM. In test mode

Pin	Symbol	Type	Pad Ref Voltage	Description
				this signal is used as test signal input.
25	SVDD	PWR		Connected to SAM power supply; used as a reference for communication with the SAM.
26	P31	IO	PVDD	General purpose IO signal. Can be configured to act either as TX line of the second serial interface or general purpose IO. In test mode this signal is used as input and output test signal.
27	P30	IO	PVDD	General purpose IO signal. Can be configured to act either as RX line of the second serial interface or general purpose IO. In test mode this signal is used as input and output test signal.
28	IRQ	O	PVDD	Interrupt request: Output to signal an interrupt event to the host (Port 7 bit 0)
29	RSTOUT	IO	PVDD	Output reset signal. When Low it indicates that the circuit is in reset state.
30	DELATT	O	PVDD	Optional output for an external 1.5 KOhms resistor connection on D+.
31	NSS	IO	PVDD	Not Slave Select. In test mode this signal is used as input and output test signal.
32	MOSI	IO	PVDD	Master Out Slave In. In test mode this signal is used as input and output test signal
33	MISO	IO	PVDD	Master In Slave Out. In test mode this signal is used as input and output test signal
34	SCK	IO	PVDD	Serial interface clock. In test mode this signal is used as input and output test signal
35	PVDD	PWR		Pad power supply
36	P33_INT1	IO	PVDD	General purpose IO signal. Can be used to generate an HZ state on the output of the selected interface for the Host communication and to enter TAMA into power down mode without resetting the internal state of TAMA. In test mode this signal is used as input and output test signal.
37	P32_INT0	IO	PVDD	General purpose IO signal. Can also be used as an interrupt source In test mode this signal is used as input and output test signal.
38	RSTPD	I	PVDD	Reset and Power Down: When High, internal current sources are switched off, the oscillator is inhibited, and the input pads are disconnected from the outside world. With a positive edge on this pin the internal reset phase starts.
39	DVDD	PWR		Digital Power Supply
40	VBUS	PWR		USB power supply.

4 OPERATING MODES

PN531 supports the following operating modes:

- Reader/Writer mode supporting ISO14443A/MIFARE® and FeliCa™ scheme
- Card Operating mode supporting ISO14443A/MIFARE® and FeliCa™ scheme
- NFC mode including 106, 212 and 424kbit/s.

The modes support different baudrates and modulation schemes. The following chapters will explain the different modes in more detail.

4.1 Reader/Writer Operating mode

The PN531 can act as a reader / writer for ISO14443A/MIFARE® or FeliCa™ cards.

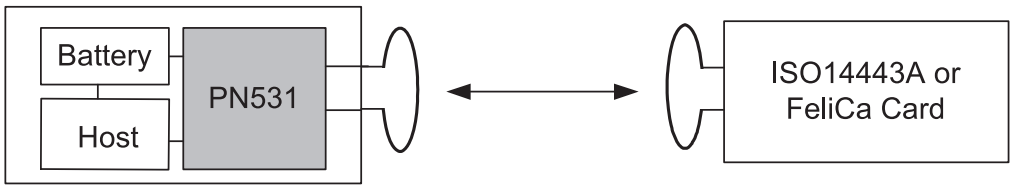


Figure 3 Reader/Writer Mode

In the reader/ writer mode the PN531 enables communication to a passive ISO14443A/MIFARE® or FeliCa™ card.

The PN531's firmware and contactless UART handle the ISO 14443A/MIFARE® and FeliCa™ protocol.

4.2 NFC MODE

NFC communication differentiates between an active and a passive communication.

- Active NFC Mode means both the initiator and the target are using their own RF field for the communication.
- Passive NFC Mode means that the target answers to an initiator command in a load modulation scheme. The initiator is active i.e. generating the RF field.

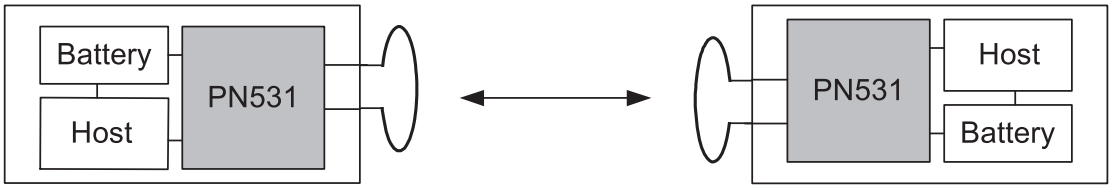


Figure 4 NFC Mode

- Initiator: generates RF field @ 13.56 MHz and starts the NFC communication
- Target: responds to initiator commands either using load modulation scheme (RF field continuously generated by Initiator) or using modulation of self generated RF field (no RF field generated by initiator)

4.2.1 ACTIVE NFC MODE

Active NFC Mode means both the initiator and the target use their own RF field to enable the communication.

- Communication Diagrams for active NFC communication

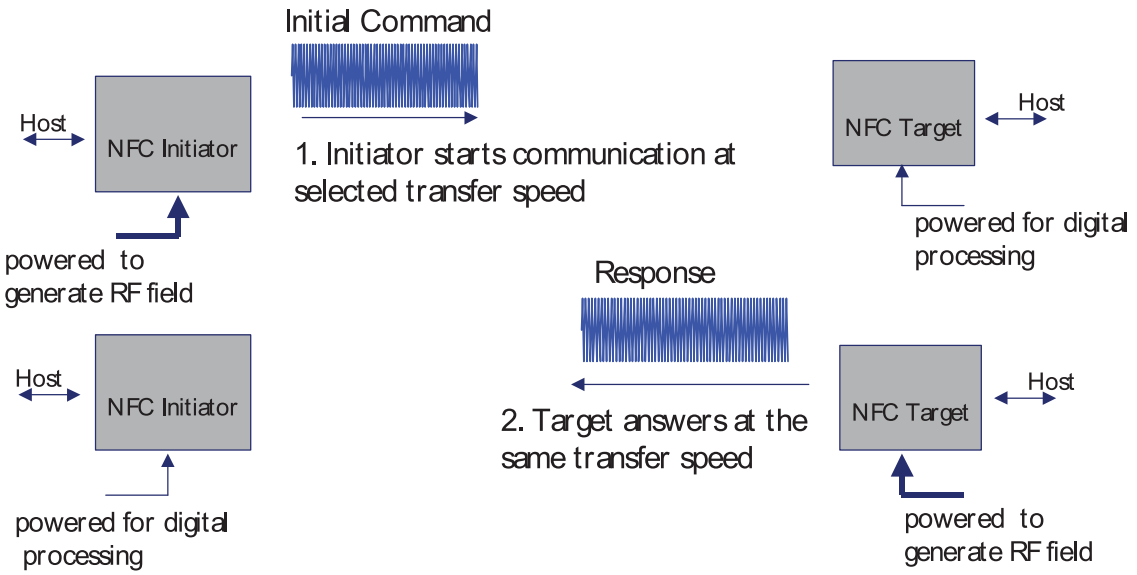


Figure 5 active NFC Mode

The PN531's firmware and contactless UART handle the NFC protocol.

4.2.2 PASSIVE NFC MODE

Passive NFC Mode means that the target answers to an initiator command in a load modulation scheme. The initiator is active i.e. generating the RF field.

- Communication Diagrams for passive NFC communication

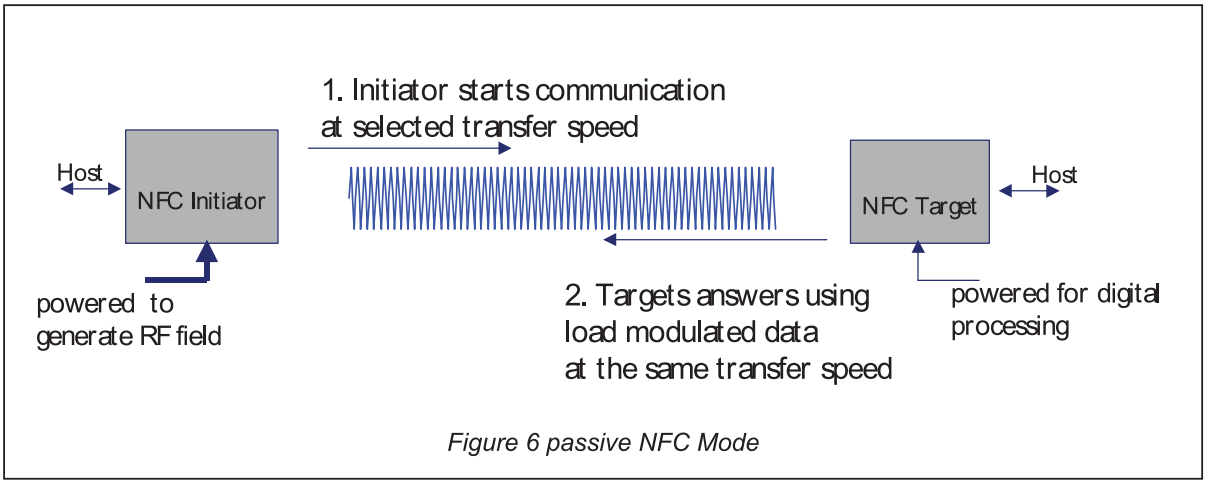


Figure 6 passive NFC Mode

The PN531's firmware and contactless UART handle the NFC protocol.

4.3 Card Operating mode

The PN531 can be addressed like a FeliCa™ or ISO14443A/ MIFARE® card. This means that the PN531 in combination with a secure µC may acts as an ISO14443A /MIFARE® or FeliCa™ card.

- Communication diagram

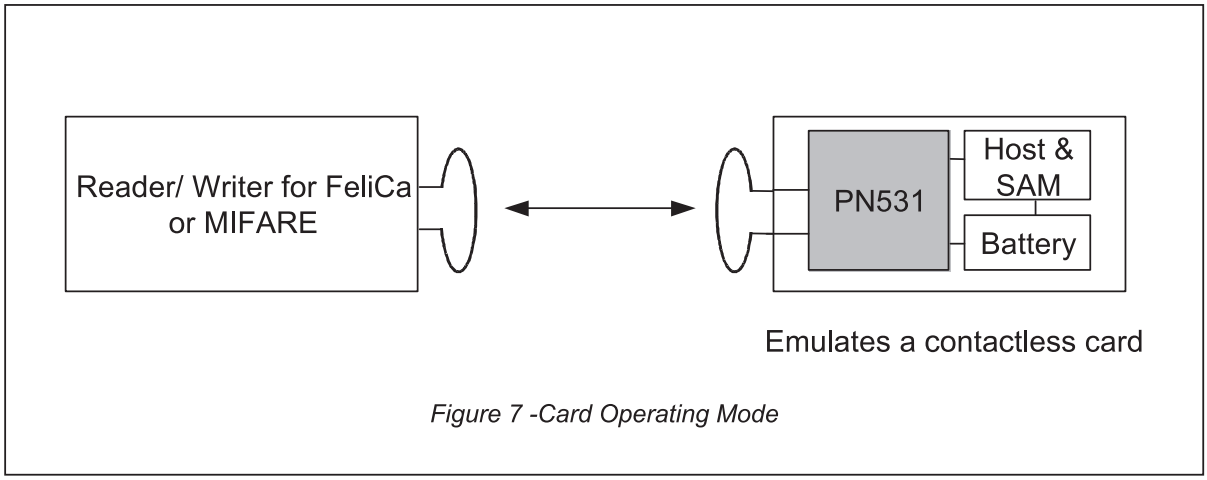


Figure 7 -Card Operating Mode

5 TYPICAL APPLICATION

5.1 Circuit Diagram

5.1.1 CIRCUIT BASED ON SPI, SERIAL UART OR I2C HOST INTERFACE

The figure below shows a typical application, where the antenna is directly connected to the PN531. The used host interface is SPI, Serial UART or I2C.

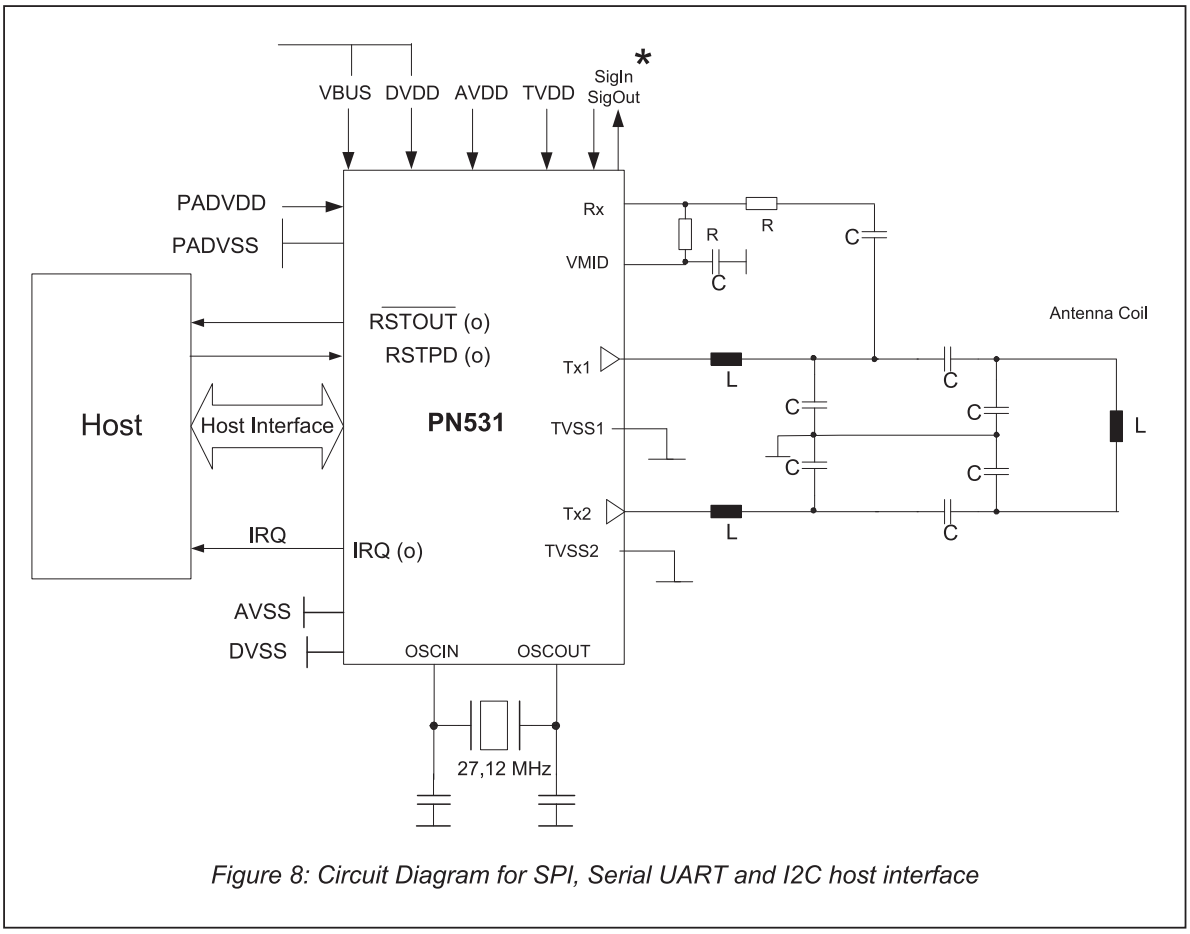


Figure 8: Circuit Diagram for SPI, Serial UART and I2C host interface

Note:

1. * Can be used in the card operating mode to connect to SAM

2. (o) Optional

5.1.2 CIRCUIT BASED ON USB HOST INTERFACE

The figure below shows a typical application where the antenna is directly connected to the PN531. The host interface is USB.

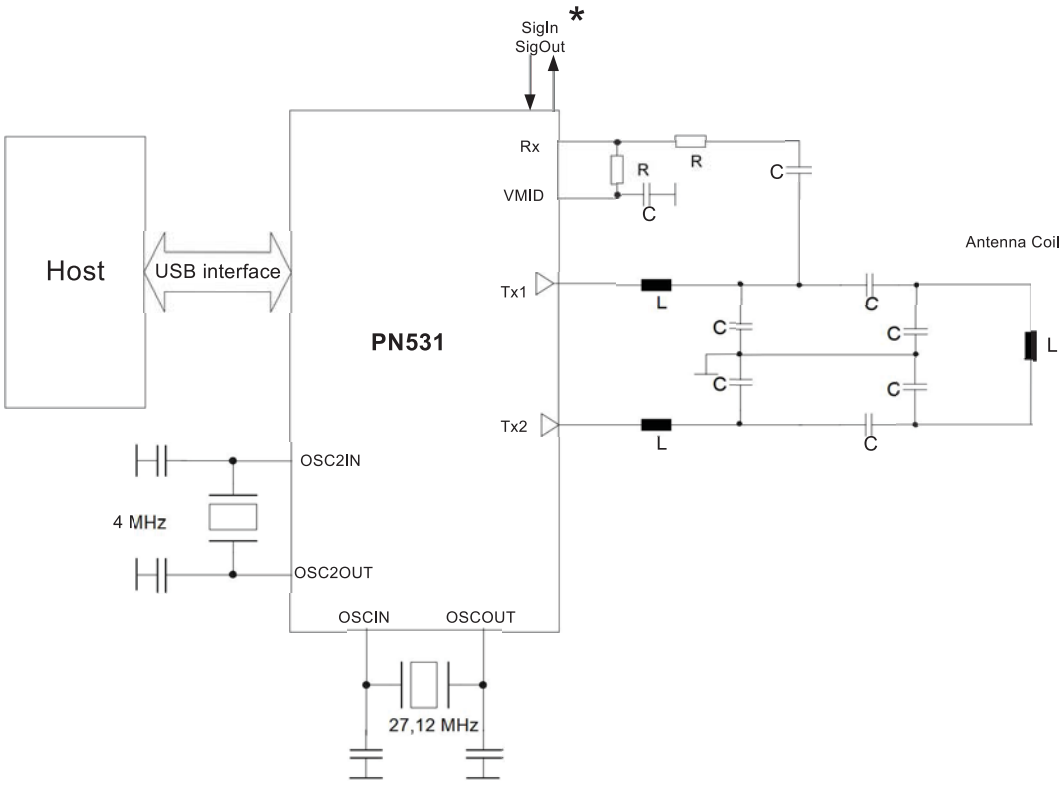


Figure 9: Circuit Diagram with USB host interface

Note:

1. * Can be used for the card operating mode to connect to SAM

6 ELECTRICAL CHARACTERISTICS

6.1 Absolute Maximum Continuous Ratings

SYMBOL	PARAMETER	MIN	MAX	UNIT
AVDD DVDD PVDD SVDD TVDD	Supply Voltages	-0.5	4.0	V
VBUS	USB Supply Voltage	-0.5	5.5	V

Table 6-1: Absolute Maximum Continuous Ratings

6.2 Operating Condition Range

SYMBOL	PARAMETER	CONDITIONS	MIN	TYP	MAX	UNIT
Tamb	Ambient Temperature		-30	+25	+85	°C
VBUS	USB Supply Voltage (USB mode)	VSS = 0V	4.2	5	5.25	V
	Supply Voltage (Non USB mode)	VBUS= DVDD VSS = 0V	2.5	3.3	3.6	V
TVDD, AVDD, DVDD	Supply Voltages	TVDD= AVDD= DVDD VSS = 0V	2.5	3.3	3.6	V
PVDD	Supply Voltage for host interface	VSS = 0V	1.6	1.8 – 3.3	3.6	V
SVDD	Supply Voltage for SAM interface	VSS = 0V	1.6	1.8 – 3.3	3.6	V

Table 6-2: Operating Condition Range

Note:

1. TVDD<3V reduces the performance (e.g. the achievable operating distance).
2. VSS represents DVSS, AVSS, TVSS1 and TVSS2

6.3 Current Consumption

SYMBOL	PARAMETER	CONDITIONS	MIN	TYP	MAX	UNIT
I_{HPD}	Hard Power Down Current (Not powered from USB)	AVDD=DVDD=TVDD=PVDD=SVDD=3V, RF level detector off			10	µA
I_{SPD}	Soft Power down Current (Not powered from USB)	AVDD=DVDD=TVDD=PVDD=SVDD=3V, RF level detector on			30	µA
I_{supend}	USB suspend Current	AVDD=DVDD=TVDD=PVDD=SVDD=3V, RF level detector on (without resistor on D+/D-)			250	µA
I_{DVDD}	Digital Supply Current	AVDD=DVDD=TVDD=PVDD=SVDD=3V, RF level detector on		15		mA
I_{AVDD}	Analog Supply Current	AVDD=DVDD=TVDD=PVDD=SVDD=3V, RF level detector on		6	tbd	mA
	Analog Supply Current	AVDD=DVDD=TVDD=PVDD=SVDD=3V, RF level detector off		3	tbd	mA
I_{PVDD}	Pad Supply Current				tbd	mA
I_{SVDD}	Pad Supply Current for SAM interface				tbd	mA
I_{TVDD}	Transmitter Supply Current	Continuous Wave, TVDD=3V		60	100	mA

Table 6-3: Current Consumption

Note:

1. TVDD depends on TVDD and the external circuitry connected to Tx1 and Tx2.
2. DVDD depends on the system configuration.
3. PVDD depends on the overall load at the digital pins.
4. SVDD depends on the overall load at the digital pins.
5. During operation with a typical circuitry the overall current is below 100 mA. Typical value using a complementary driver configuration and an antenna matched to 40 Ohm between TX1 and TX2 at 13.56 MHz.

7 REVISION HISTORY

REVISION	DATE	DESCRIPTION
2.0	February 2004	Second published version, change to public
1.0	April2003	First published version

Table 7: Document Revision History

8 DEFINITIONS

Data sheet status	
Objective specification	This data sheet contains target or goal specifications for product development.
Preliminary specification	This data sheet contains preliminary data; supplementary data may be published later.
Product specification	This data sheet contains final product specifications.
Limiting values	
Limiting values given are in accordance with the Absolute Maximum Rating System (IEC 134). Stress above one or more of the limiting values may cause permanent damage to the device. These are stress ratings only and operation of the device at these or at any other conditions above those given in the Characteristics section of the specification is not implied. Exposure to limiting values for extended periods may affect device reliability.	
Application information	
Where application information is given, it is advisory and does not form part of the specification.	

9 LIFE SUPPORT APPLICATIONS

These products are not designed for use in life support appliances, devices, or systems where malfunction of these products can reasonably be expected to result in personal injury. Philips customers using or selling these products for use in such applications do so on their own risk and agree to fully indemnify Philips for any damages resulting from such improper use or sale.

Philips Semiconductors - a worldwide company

Contact Information

For additional information please visit **http://www.semiconductors.philips.com**.Fax: **+31 40 27 24825**
For sales offices addresses send e-mail to: **sales.addresses@www.semiconductors.philips.com**.

Let's make things better.

Philips Semiconductors

PHILIPS

EXHIBIT G

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

TRIDINETWORKS LTD., Plaintiff, v. NXP-USA, INC. and NXP B.V., Defendants.	No. 1:19-01062-CFC-CJB
TRIDINETWORKS LTD., Plaintiff, v. SIGNIFY NORTH AMERICA CORPORATION and SIGNIFY NETHERLANDS B.V., Defendants.	No. 1:19-01063-CFC-CJB
TRIDINETWORKS LTD., Plaintiff, v. STMICROELECTRONICS, INC., and STMICROELECTRONICS INTERNATIONAL N.V., AND DOE-1 d/b/a "STMICROELECTRONICS," Defendants.	No. 1:19-01064-CFC-CJB **Declaration of Anthony G. Rowe**

I, ANTHONY G. ROWE, declare the following under penalty of perjury:

1. I submit this declaration to comment briefly on certain new matter presented in Dr. Caloyannides' reply declaration in this case.

2. As I said in Par. 45 of my prior declaration: "In my view, the advance represented by the '276 patent, in networking industrial and/or home automation devices, lies in building in the capability to download data to the device before it is initialized, to configure devices to the designated design, while in an unpowered state, state, prior to their initialization, so that when deployed and later initialized they automatically bring themselves up on the network, in their intended position and role." Rowe Decl. ¶ 45.

3. Dr. Caloyannides' Reply recycles many of the same references as his opening declaration, without responding to my criticisms of those references. In addition, however, he adds a new one, the Philips PN531 chip. He puts forth the following, seeking to align the PN531 with the "Configuration Adapter" of the '276 patent claims:

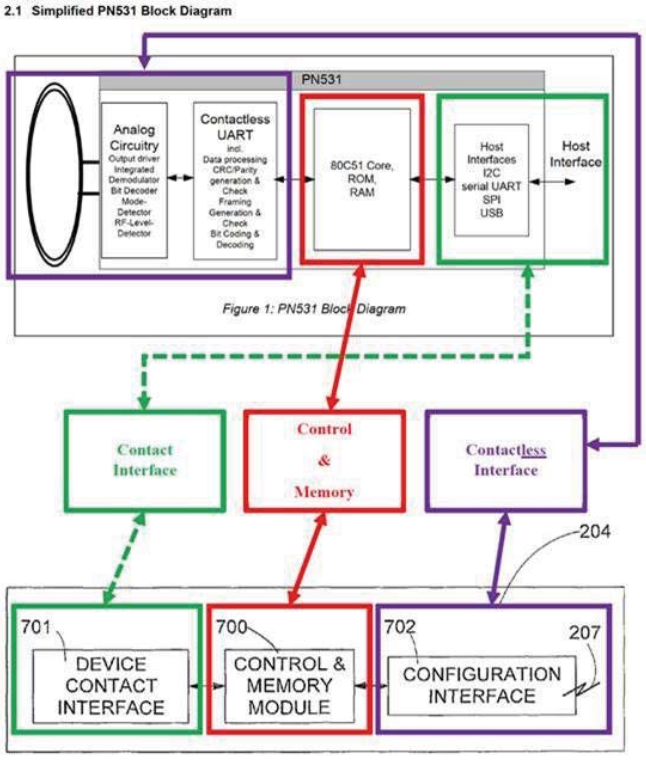


Fig. 7

4. This contention is considerably off base. To function in the manner I described in par. 45 of my declaration, the device in question must have the on-board capability to persist the

data it stores while unpowered, so that when "later initialized" it can use that data to "automatically" bring itself up on the network. Dr. Caloyannides' diagram shows, within the PN531, ROM and RAM. The ROM is a Read-Only Memory and cannot be written to. The RAM is Random Access Memory, which is a volatile memory that loses its data when power is removed. The PN531 is a data pipe that lacks persistent internal storage and needs a host controller and power to operate. It falls considerably short of what is required to function as a configuration adapter in the claimed invention.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on January 28, 2021.

ANTHONY G. ROWE